Broadview
www.broadview.com.cn

“十一五”国家重点图书出版规划项目

Microsoft Most Valuable Professional

安全技术大系

Windows 7 安全指南

刘晖 汤雷 张诚 等编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

- android与iphone及ipad开发书籍 ----------持续不断更新中.....
- c、c++、c#语言pdf书籍及vip视频教程 c、c++、c#、vc等-------持续不断更新中.....
- delphi《书籍》及《视频》教程 ----------持续不断更新中.....
- E网情深VIP系列视频教程 黑客破解菜鸟修练班，VB编程学习班，仿站学习培训，免杀培训，个人系统攻防系列教程，服务器搭建学习班，PHOTOSHOP平面设计班，基础制作论坛（论坛网站搭建），网赚系列教程，网站建设教程，网站漏洞基础，远程控制教程，软件破解班，脚本漏洞提权班
- IT9网络学院VIP系列视频教程 免杀培训班，VMware虚拟机，零基础学习C语言，网游外挂开发精品系列语音教程（外挂教程学习必备研修31课全），VB语言教程30课全，Delphi编程到精通，远程控制软件，加密解密班，网络安全与黑客攻防培训，从入门到精通完整系统化学习C++编程，从入门到精通零基础学习汇编，wordpress教程(个人博客系统49课全)，外行人做易语言盗号和钓鱼程序语音教程 网址：WLSAM168.400GB.COM
- Java书籍 ----------持续不断更新中.....
- photoshop、CorelDRAW、AutocAD等图像处理书籍及vip视频教程 -------持续不断更新中.....
- powerbuilder书籍大全
- Visual Basic语言vip视频教程及pdf书籍 ----------持续不断更新中.....
- windows、linux系统开发、系统封装等pdf书籍及VIP视频教程 ----------持续不断更新中.....
- 《3DS Max》pdf书籍
- 《汇编语言》、《反汇编》及《调试》pdf书籍及vip视频教程 ----------持续不断更新中.....
- 《电子书、电子书、还是电子书》pdf专题库 编程开发，家居美食，儿童益智，人物传记，增强记忆，快速阅读
- 信息系统项目管理师、网络工程师、系统分析师等软考类书籍
- 华中红客系列vip视频教程 脚本攻防培训班，源码免杀培训班，Css语言培训班，C语言，Dreamweaver网页设计，html网页设计培训班，PC安全班， php脚本语言培训班，VMWare虚拟机专题，webshell提权培训班，防站教程，零基础免杀培训班，刷钻速成班，脱壳破解班，外挂编写班，网络赚钱培训班，网站入侵培训班
- 外挂、驱动、逆向及封包视频教程 郁金香、独立团、夜猫论坛、天都吧、看流星论坛、一切从零开始等等
- 安全中国系列vip视频教程 易语言软件编程培训班，ASP.net网站开发项目实战培训班
- 我的收藏
- 按键精灵及TC脚本开发软件视频教程 ----------持续不断更新中.....

当前位置：/《电子书、电子书、还是电子书》pdf专题库

文件名 ⇕

PDF电子书专题库，内容详尽，每天不断更新！！

- 办公类软件使用指南
- 医学
- 历史人物传记
- 哲学宗教
- 外语资料（除英语外） （除英语外）
- 官场类小说
- 建筑工程类
- 情感生活类小说
- 政治军事
- 教育学习科普大全
- 文学理论
- 智力开发、增强记忆、快速阅读技巧大全
- 社会生活
- 科学技术
- 程序编程类
- 经济管理
- 网络安全及管理
- 网赚系列
- 美食小吃烹饪煲汤大全
- 课外读物

本网盘内容太多，持续不断更新，发布各类视频教程、pdf书籍，包括破解、加解密、外挂辅助制作，易语言培训教程、编程语言、网页制作等等，教程及书籍仅用于学习,如用于商业或非法用途的后果自负！

网址：WLSAM168.400GB.COM

- VIP培训教程，易语言黑月VIP视频教程，天都网易语言系列培训教程(100集全)，集中营易语言学习视频(80集)
- 棉猴系列vip视频教程 gh0st远控控制源码讲解教程，套接字编程，DLL程序编写，键盘监听驱动程序编写，驱动基础教程，AsyncSelect模型QQ程序教程，C++语言入门基础，NB5.5源码分析教程
- 游戏开发pdf书籍 ----------持续不断更新中.....
- 炒股投资pdf书籍及视频教程 短线高手系列，短线天王系列，操盘论道系列，翻倍黑马，看盘快速入门，庄家手法大曝光等等。 网址：WLSAM168.400GB.COM
- 热门小说集中营 傲世九重天，网游之三国时代，武动乾坤
- 甲壳虫VIP教程全集 asp教程，Delphi培训班，FLASH培训班，Java培训班，linux培训班，PHP培训班，源码免杀班，甲壳虫C++，脚本功防班，免杀班初、中、高级班，破解班，源码免杀班，脱壳班，易语言培训班，无特征码免杀，网站架构培训班，外挂高级班，外挂初级班第1、2部
- 破解、免杀、入侵、脱壳、攻防及漏洞分析系列VIP视频教程（80多部） 天草、黑客动画吧等等--------持续不断更新中....
- 网站建设相关的pdf书籍及各种vip视频教程 ----------持续不断更新中.....
- 网赚、淘宝系列vip视频教程 网赚30天新人魔鬼训练，屠龙网赚团队vip课程，站长大学网赚视频（50课全），图腾团队日赚1000元竞价行销教程，屠龙团队淘宝宝贝卖疯系列，站群网赚系列，淘宝开店视频，红星挂机日赚10元，百万流量系列，漂流瓶圣手全自动挂机引，贴吧邮件定向营销疯狂成交量月入万元
- 英语学习资料百科大全 不断更新。。。
- 饭客论坛系列VIP视频教程 脚本入侵班，黑客之免杀教程，易语言教程，无线网络攻防教程，入侵教程，delphi系列教程，黑客基础入门
- 黑客书籍 有关黑客、安全、加解密技术等等----------持续不断更新中.....
- 黑手安全网VIP系列视频教程 DIV+CSS网页布局，Dreamweaver教程，flsah动画教程，photoshop教程，跟我一起学C++课程，抓鸡
- 黑鹰、黑基、黑防、黑盾vip系列视频教程 破解提高班66课全，SQL注入，ASP注入教程，完完全全学会抓肉鸡，脱壳破解教程50课全，提权班，C语言特训班26讲全，黑客脚本特训班，黑客工具特训班，dedecms仿站教程，VC编写远控30课全，网页美工特训班，木马免杀特训班，驱动开发技术VIP培训班，外挂破解等等。

- [电脑世界的通关密语：电脑编程基础].(杉浦贤).滕永红.扫描版.pdf
- [程序语言的奥妙：算法解读（四色全彩）].(杉浦贤).李克秋.扫描版.pdf
- [差错：软件错误的致命影响].(帕伯斯).邝宇恒等.扫描版.pdf
- [算法之道（第2版）].邹恒明.扫描版.pdf
- [O'Reilly：深入学习MongoDB].(霍多罗夫).巨成等.扫描版.pdf
- [深入浅出WPF].刘铁猛.扫描版.pdf
- [Go语言·云动力（云计算时代的新型编程语言）].樊虹剑.扫描版.pdf
- [精通.NET互操作：P/ Invoke、C++ Interop和COM Interop].黄际洲等.扫描版.pdf
- [编程的奥秘：.NET软件技术学习与实践].金旭亮.扫描版.pdf
- [O'Reilly：学习OpenCV（中文版）].(布拉德斯基等).于仕琪等.扫描版.pdf
- [Go语言编程].许式伟等.扫描版.pdf 网址：WLSAM168.400GB.COM
- [MySQL技术内幕：SQL编程].姜承尧.扫描版.pdf
- [Tomcat权威指南（第2版）].(布里泰恩等).吴豪等.扫描版.pdf
- [Ext江湖].大漠穷秋.扫描版.pdf
- [IT名人堂·Oracle DBA突击：帮你赢得一份DBA职位].张晓明.扫描版.pdf

Total: 77 1 2 3 4 5 6 ›

博文视点·IT出版旗舰品牌
技术凝聚实力·专业创新出版
Broadview
www.broadview.com.cn

安 全 技 术 大 系

Windows 7 安全指南

计算机十大安全准则

1. 如果攻击者能够说服你在自己的计算机上运行他的程序，那么该计算机便不再属于你了。
2. 如果攻击者能够在你的计算机上更改操作系统，那么该计算机便不再属于你了。
3. 如果攻击者能够不受限制地实地访问你的计算机，那么该计算机便不再属于你了。
4. 如果你允许攻击者上传程序到你的网站，那么该网站就不再属于你了。
5. 再强大的安全性也会葬送在脆弱的密码手里。
6. 计算机的安全性受制于管理员的可靠性。
7. 加密数据的安全性受制于解密密钥的安全性。
8. 过时的病毒扫描程序比没有病毒扫描程序好不了多少。
9. 绝对的匿名无论在现实中还是在网络上都不切实际。
10. 技术不是万能药。

上架建议：操作系统>Windows>安全

ISBN 978-7-121-11211-9

9 787121 112119 >

定价：50.00元

责任编辑：李 冰
责任美编：侯士卿

“十一五”国家重点图书出版规划项目

Windows 7 安全指南

刘晖 汤雷 张诚 等编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

在客户端操作系统领域，Windows 的使用率是最高的。对于微软最新的 Windows 7 操作系统，虽然可以说是目前安全性最高的操作系统，但受限于所谓的“木桶原理”，如果在使用中不注意，依然可能遇到潜在的安全隐患，并可能导致严重后果。

对于目前较新版本的 Windows 系统，已经将安全性放在了第一位。系统中的大部分默认设置都是以保证安全为前提的。然而安全性和易用性就像鱼和熊掌，永远不可兼得。因此，在实际使用的过程中，我们可能还需要根据具体情况调整设置，提高易用性。如何在这两者之间进行取舍？如何能够在提高易用性的同时尽可能保证安全？这就是本书要介绍的内容。

本书将从具体应用角度出发，介绍 Windows 7 系统在不同场合需要注意的安全选项，介绍此类选项的用途，以及建议的设置方式。另外，本书还将从更高层面的原理和原则进行介绍，这些内容不仅适合 Windows 7，还可用于其他任何主流的客户端操作系统。

本书适合对 Windows 系统有基本了解和使用经验，并且对系统以及软件的安全性不够放心的人群。相信通过阅读本书，您将对 Windows 7 的安全性有一个全新的认识，并且能更好地将其应用到实际使用中，不仅可以保护您的系统，而且可以让具体的使用更加便利、简单。

图书在版编目（CIP）数据

Windows 7 安全指南 / 刘晖等编著. —北京：电子工业出版社，2010.8（安全技术大系）
ISBN 978-7-121-11211-9

Ⅰ. ①W… Ⅱ. ①刘… Ⅲ. ①窗口软件，Windows 7—安全技术 Ⅳ. ①TP316.7

中国版本图书馆 CIP 数据核字（2010）第 122560 号

责任编辑：李 冰
印　　刷：北京智力达印刷有限公司
装　　订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1092　1/16　印张：26.25　字数：621.6 千字
印　　次：2010 年 8 月第 1 次印刷
印　　数：4000 册　　定价：50.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

很多人都认为，Windows 操作系统的安全性太差。其实，对于新的 Windows 操作系统，例如 Windows Vista/7，系统的安全性已经得到了空前的加强，然而依然有很多人在使用这些操作系统的时候因为安全问题而受到损失，到底是什么原因？

其实在计算机安全方面，也一直存在“木桶原理”，就像一只用木板拼成的木桶，桶里能装多少水，并不取决于最长的木板，而取决于其中最短的木板。可能操作系统本身已经很安全，但因为使用的人缺乏安全意识，也有可能导致操作系统在提高安全性方面所做的全部努力付之东流。

在现在的 Windows 操作系统中，几乎所有选项的默认设置都是以保证安全性为前提的。然而安全性和易用性永远都是对立的，如果要实现更高的安全性，在易用性方面肯定会大打折扣。因此，很多人在使用过程中为了贪图方便，往往会修改一些默认的系统设置，导致系统变得不够安全。而一旦遇到安全性问题，往往会觉得这是操作系统做得不好，并不会想到是因为自己修改的设置导致了一系列的不安全问题。

对于使用 Windows 的大部分一般用户来说，他们并不需要对计算机有多么高深的了解，他们只需要像使用一般电器那样打开计算机，然后学习、工作或者娱乐，并在用完之后直接关掉就可以，Windows 可以很好地满足这些人的需求。也许有更加安全的操作系统，但对于大部分用户来说，这类系统无论是安装、设置还是使用，都存在不小的难度，甚至可能根本无法在这些操作系统上完成自己需要的工作。因此，大部分人依然在使用 Windows，并希望努力让 Windows 变得更安全，或者至少不要因为自己的疏忽带来安全问题。

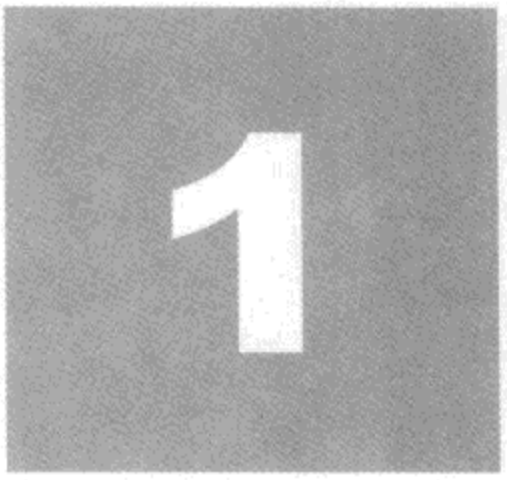
一般来说，如果希望自己的计算机更安全，我们应该从以下几个方面着手：

- 随时保持操作系统和应用程序安装了最新的补丁：现在的软件越来越复杂，存在安全漏洞也是在所难免的。因此，无论是操作系统还是一般的应用程序，只要有安全方面的更新，就应该尽快安装，只有这样才能保护计算机不被入侵或攻击。
- 给每个使用电脑的人创建自己的账户，并设置强密码：这样，每个人的使用环境将会被隔离起来，并且可以根据不同的需要给不同用户指派不同的特权，这样才能保证每个用户只能做自己需要的工作，而不会“越权”。同时强密码的存在也可以保证系统和数据不被未经授权的人访问。
- 安装反病毒软件、网络防火墙及反间谍软件：这三类软件可以保护我们的系统不被攻击和感染，但不要忘记经常更新这类软件的定义文件，只有这样才能监测到最新类型的攻击或病毒。
- 对于电子邮件中的可疑附件，绝对不能轻易打开：很多病毒在通过电子邮件传播，有时候可能看似来自朋友的邮件，其实可能是对方感染病毒后不知情的情况下发送的。因此，在收到任何人发来的邮件时都要谨慎，在打开之前最好使用反病毒软件彻底检查。

目　录

第 4 部分　其他安全问题

窍门目录



第 1 部分
Windows 安全

对于计算机来说，操作系统是其他所有应用的基础。无论使用计算机做什么，如果操作系统不安全，那么其他应用和数据就会受到影响。因此，对于需要更安全的计算环境的用户，首先需要保证 Windows 的安全。

然而长久以来，因为各种原因，很多人对 Windows 的安全性有一个误解，认为和其他操作系统相比，Windows 不够安全，其他系统更安全。其实这个观点在很大程度上都是站不住脚的。

首先，我们必须知道，Windows 是全世界使用率最高的操作系统，很多人都在研究和破解 Windows 的各种安全功能，以达到各自的目的。设想这样一种比较极端的情况：有一种全新的操作系统，存在比较严重的漏洞，但全世界只有一两个人在使用这个系统，并且主要用于娱乐用途，那么会有人对这种操作系统的漏洞感兴趣吗？很显然，不会，因为没有价值。

那么 Windows 呢？情况有些复杂。很多人在用 Windows，我们会在 Windows 下进行网络理财、股票交易，会在 Windows 下处理公司的财务数据，会在 Windows 下撰写新计划的企划书，会在 Windows 下玩网络游戏，打造可以卖钱的极品装备……总之，在 Windows 下进行了太多有价值的应用。因此，研究 Windows 各种功能和漏洞的人最多，进而，Windows 上出现的安全问题也最容易被怀有恶意的人利用，这些因素更让 Windows 显得不够安全。

其次，Windows 是由人编写的一套非常庞大的操作系统。而只要是人，就难免犯错误，再加上数量庞大的代码，因此，Windows 下暴出安全漏洞也并不奇怪。其实其他任何软件产品也是如此，只不过有些软件的用户数量太少，问题不那么突出罢了。不过好在微软有一套相当成熟的补丁管理机制，可以在发现新的安全漏洞后的最短时间里发布相应的补丁程序。我们只需要及时安装新的补丁程序，就可以将风险扼杀在摇篮中。

最后，为了保证一定的易用性，在 Windows 中，很多默认的设置都是不够安全的。虽然在 Windows Vista/7 中的这种情况有所好转，不过问题依然存在。更重要的是，系统的安全性在很大一部分情况下都取决于使用这套系统的人，不管多安全的操作系统，如果让不懂技术的人使用，都有可能因为改变了设置或者错误的使用习惯而导致原本安全的系统变得不再安全。

因此，就算选择使用 Windows，也不用因为上述内容而沮丧。因为通过本书，我们会了解到怎样进一步提高 Windows 的安全性，同时，本书还会介绍怎样让我们在 Windows 下进行的其他操作更安全。

CHAPTER

1

第 1 章　安装和设置

很多人认为 Windows 的安全设置是在安装好系统之后才进行的，其实不然。要知道，从操作系统的安装开始，很多因素都有可能影响到系统和其他程序的安全性。举例来说，如果安装系统所用的安装文件被病毒感染或者被第三方恶意修改，那么这样安装的系统将存在先天不足的缺陷，虽然可能不至于导致系统无法使用，但安全隐患肯定是存在的。另外，如果安装的某个设备驱动有问题，不仅可能影响到系统安全性，甚至可能导致整个系统崩溃。

因此，在安装操作系统之前，最好能花一些时间注意这些问题，而这也正是本章的主要内容。

1.1　安装前的准备工作

在本节中将了解到：如何通过选择合适的安装介质安装出一个更加安全的系统，以及如何将补丁和更新程序直接集成到 Windows 的安装文件中，这样安装好的系统就直接带有各种更新程序，避免了装好系统才进行更新的麻烦。

1.1.1　安装介质的选择

对于大部分购买了零售版 Windows 或者购买预装了正版 Windows 的品牌机用户来说，这部分内容可以跳过，因为正版 Windows 系统几乎不存在这类问题。但对于使用盗版或者“伪正版”的用户，这是一个很重要的问题。

虽然提倡使用正版，但事实上，依然有很多人因为各种原因在使用盗版软件，其中就包括 Windows。市面上各种盗版 Windows 产品的种类非常多，例如，号称某企业或者某政府机构的专用免激活大客户版，或者以某论坛或网站名义制作的 Ghost 镜像等。很多人贪图方便，使用这些盗版，尤其是 Ghost 镜像，因为使用起来很便捷，只要几分钟就可以安装好操作系统和所有常用的程序。

虽然传播这些软件的人大部分都只是为了方便大家使用，而不是为了私利，但在这背后却隐藏着巨大的危险，因为有少数人在借助这些东西非法赢利。例如，前一段时间新闻

里报道，某个非常著名的 Ghost 镜像版本的 Windows XP 打包者被抓捕，并且发现该打包者的软件内通过收费的方式捆绑其他软件，非法获利上百万，而其中捆绑的软件大部分都有一些不好的“恶意行为”，使用了这种系统的人可能面临系统中弹出广告、隐私或机密信息被泄露，甚至系统功能无法正常使用等各种危险。

其实这些问题还不是最严重的，有些 Ghost 镜像中甚至建立了隐藏的账户，并开放了某些网络端口，这样，制作这些镜像文件的人将可以通过开放的端口，使用隐藏账户连接我们的系统，暗地里进行一些不好的操作。这才是对系统和数据安全危害最大的！

因此，在选择操作系统的安装介质时一定要小心谨慎，尽量不要因为贪图便宜或方便而导致更麻烦的后果。

1.1.2　将补丁和更新集成到安装文件中

什么是补丁，补丁都有哪些类型，为什么要安装补丁，又怎样才能获得并安装补丁，这些内容会在本书第 4 章“补丁和更新”中详细介绍。这里只介绍怎样将补丁集成到 Windows 的安装文件中，这样安装好的系统就已经包括了集成的补丁，避免了装好系统后花大量时间进行更新的麻烦。

在 Windows 7 中，因为修补方式的改进，用很简单的操作就可以将所有的更新程序集成到安装文件里。因为在撰写这本书的时候，Windows 7 还没有发布任何 Service Pack（简写为 SP），因此，在这里只能以 Hotfix 补丁为例来介绍。在 Windows 7 的 SP1 发布后，就可以使用类似的方法将 Service Pack 集成到安装文件中。

要将更新程序和补丁集成进 Windows 7 的安装文件，我们需要准备下列工具和材料：

- DVD 刻录机和 DVD 刻录盘，或者使用普通的 U 盘，因为 Windows 7 可支持从 U 盘引导安装（具体做法请参考下文）。
- 原始版本的 Windows 7 安装光盘。
- Windows 7 的更新程序和补丁，这些文件可以在 http://tinyurl.com/ybop2yj 中下载，或者也可以使用下文介绍的 WUD 工具进行批量下载。
- 用于将更新整合到 Windows 安装文件，以及对安装文件进行定制的工具 Win Integrator，其下载地址为 http://tinyurl.com/yephvxj。

如何下载 Windows 7 所需的更新程序？其实也有比较简单的办法，通过使用网上流传的一些小工具，我们可以将所有需要的更新一次性下载下来。此处推荐使用 Windows Updates Downloader（下文简称为 WUD），这是一个免费的工具，我们只要准备好合适的列表文件，即可下载微软所有产品的更新程序。首先请访问 http://tinyurl.com/cuhe86，并单击页面顶部的“Program Files”链接，随后出现的页面中将列出所有可供下载的版本。

在撰写本书时，这个工具的最新版是 2.5 Build 1000 版，下文将以该版本为例进行介绍。下载并安装该工具，随后还需要提供不同产品的列表。WUD 工具实际上是一个下载器，单纯的该工具并不能下载任何内容。而网络上很多人提供了针对微软不同产品的下载列表，

这个列表实际上可以理解为更新的清单，其中列出了不同操作系统所需的更新数量、类型、简介，以及下载地址。只有使用 WUD 加载了某个列表后，才能开始下载。对于 Windows 7 系统，可以在 http://tinyurl.com/ydum4od 处下载到最新的 x86 以及 x64 版本的下载列表，并且该列表会每月更新，因此，用户总是可以下载到最新的版本。

从上述地址下载到的列表是.ulz 格式的，安装 WUD 后，直接双击这样的文件，即可启动 WUD 软件，并加载该列表，随后可以看到如图 1-1 所示的界面。

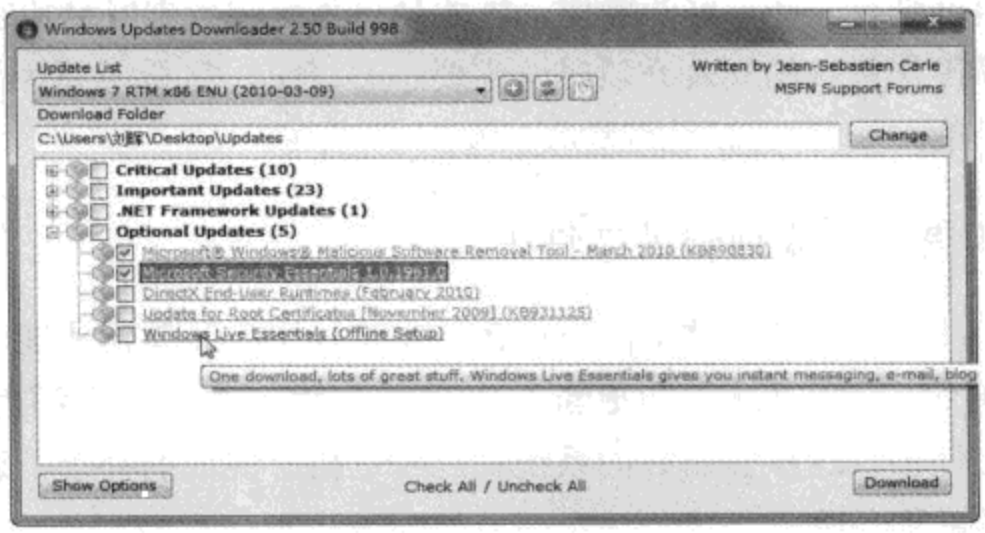


图 1-1　从列表中选择要下载的更新

如果曾经加载过多个列表，那么可以从窗口顶部的“Update List”下拉菜单中选择要使用的列表，本书所选的是针对 32 位 Windows 7 RTM 的列表。随后还可以通过右上角的“Change”按钮指定下载下来的文件的保存位置。窗口的中央部分则列出了列表所包含的内容，共分为四个部分：Critical Updates（关键更新）、Important Updates（重要更新）、.NET Framework Updates（.NET Framework 更新）、Optional Updates（可选更新）。对于每个类别，展开后可以看到具体的每个更新，将鼠标指针指向它后还可以看到详细的描述。对于希望下载的更新或某个类别的所有更新，只要单击对应的复选框即可。这里需要提醒一点，Windows 7 是完全语言中性的，也就是说，所有语种的 Windows 7，在绝大部分情况下都可以共用相同的更新程序，除非某个更新解决的是特定语种 Windows 中存在的问题，否则该列表就可以下载到 Windows 7 所需的全部更新。

选择要好下载的内容后单击“Download”按钮，WUD 会自动开始下载，并将下载的文件保存到指定的目录中（如图 1-2 所示）。

针对不同的内容，下载回来的更新程序可能使用了不同的扩展名。例如，有些文件使用了.msu 扩展名，这种文件可以直接使用 Win Integrator 整合到安装文件中，但有些文件可能使用.exe 扩展名，此类文件无法直接整合。不过，好在 Windows 7 的绝大部分更新都是.msu 格式的。

STEP 01 运行 Win Integrator（下文简称为 WI），该工具的大部分操作都是通过选项卡进行的，但在第一个选项卡上需要首先指定 Windows 7 安装文件的原始位置。请单击“Select”按钮，然后选择放入安装光盘的光驱，或保存了安装文件的文件夹。如果所选文

件中包含多个 Windows 7 版本的映象[①]，则要选择自己需要使用的版本（如图 1-3 所示）。

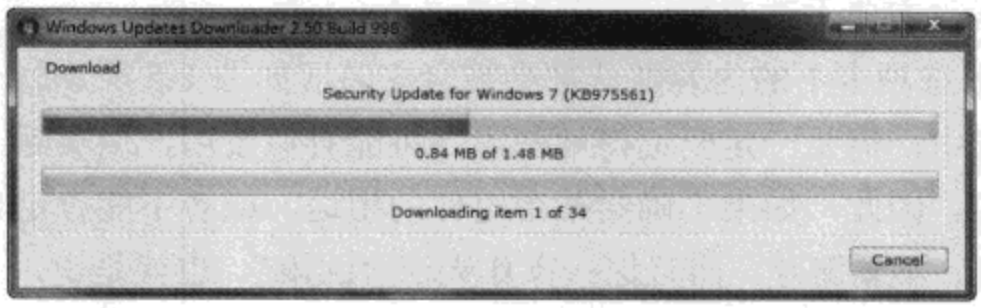


图 1-2　下载所有选中的更新

STEP 02 随后打开“Updates”选项卡，在这里可以添加之前使用 WUD 批量下载下来的更新文件。请单击“Open”按钮，并将所有需要整合的更新文件（.msu 格式）都添加进来（如图 1-4 所示）。

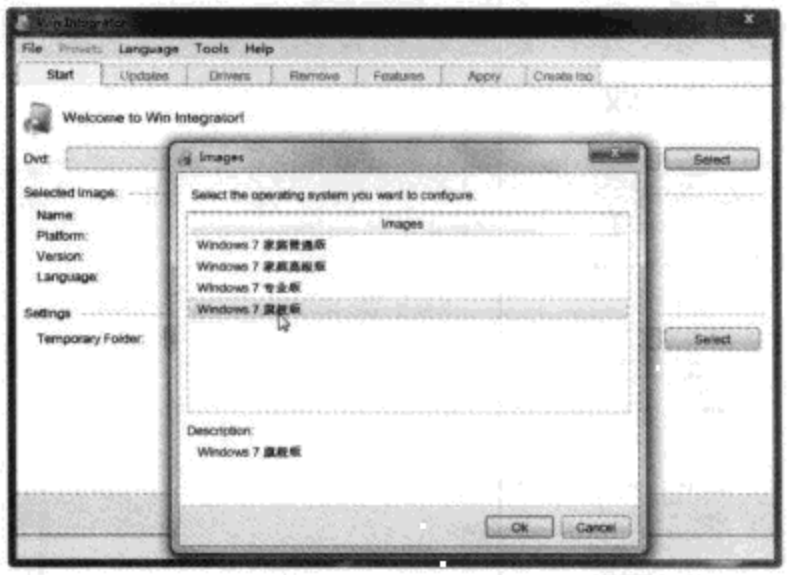


图 1-3　指定安装文件的位置并选择版本

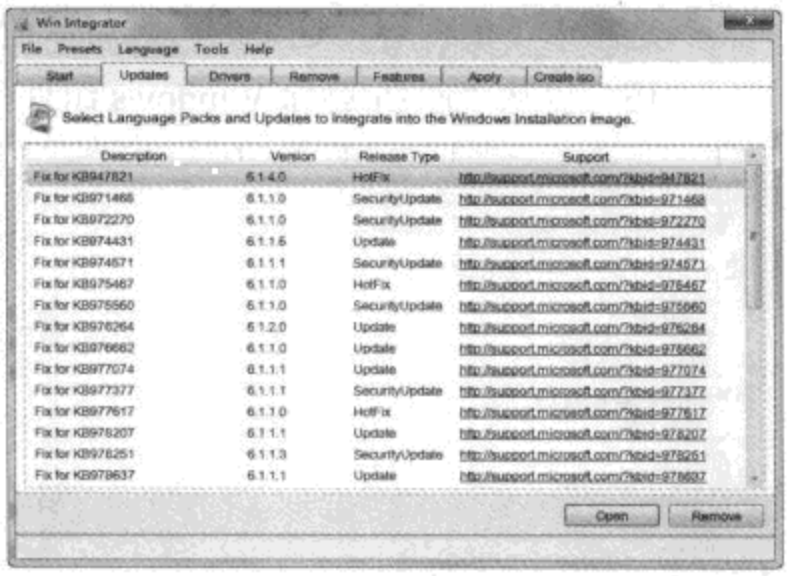


图 1-4　添加好的更新程序

STEP 03 打开“Create iso”选项卡，为 ISO 文件输入卷标，并单击右下角的“Create iso”按钮，程序会利用原始文件，以及添加和修改的内容新建一个 ISO，并保存到我们指定的位置。

至此，已经可以将所有必要的安全更新都整合到 Windows 7 安装文件中。不过 WI 的功能还远不止这么简单，我们还可以根据需要，对安装文件进行更多的定制。上述操作没有提到的选项卡以及各自的用途如下：

---

① 注意，由于采用了映象安装的方式，结合单实例存储等技术，一张 Windows 7 安装光盘实际上可以包含多个版本的安装文件。但使用零售版光盘安装时会发现，并不能选择要安装的版本，而且也不能像 Windows Vista 那样通过输入不同的序列号，用同一张光盘安装出不同的版本。其实零售版 Windows 7 光盘一样包含了多个版本，不过通过技术手段屏蔽了这种做法，无法直接安装。为了解决这一问题，可将光盘“Sources”目录下的“ei.cfg”文件删除，这样以后进行安装时，安装程序将提供选择列表，列出不同的版本供我们根据实际需要选择（这一点与 Windows Vista 不输入序列号直接安装后的效果一致）。不过，在使用 WI 进行整合的时候，必须选择一个自己要使用的版本，并且这样处理过的安装文件将不再包含多个版本的内容。

- Drivers：用于将驱动程序加入安装文件，这样在安装好系统后，所有的设备都可直接使用，不再需要手工安装设备驱动。
- Remove：该选项卡下的内容默认都会被会安装（如图 1-5 所示），如果不希望安装，可以将其选中。但是一定要记得某些组件可能看似没用，但实际上自己的正常操作还是需要的。因此，如果不确定某个组件的用途，或者不能肯定自己是否需要，建议将其保留，不要删除。而且这一操作无法“回滚”，也就是说，一旦在安装系统时将某个组件排除，后来发现自己需要这个组件时，将无法单独安装，可能需要重装整个系统。
- Features：这里对应了 Windows 7 控制面板添加或删除 Windows 组件功能所能添加和删除的内容（如图 1-6 所示）。如果自己需要使用某个默认不被安装的组件（例如 Telnet 客户端），可以在这里选中，并在安装系统的过程中自动安装。相比 Remove 选项卡下的内容，这里的内容可以放心地添加或删除，如果有必要，在装好系统后还可以从“添加/删除 Windows 组件”窗口中修改。

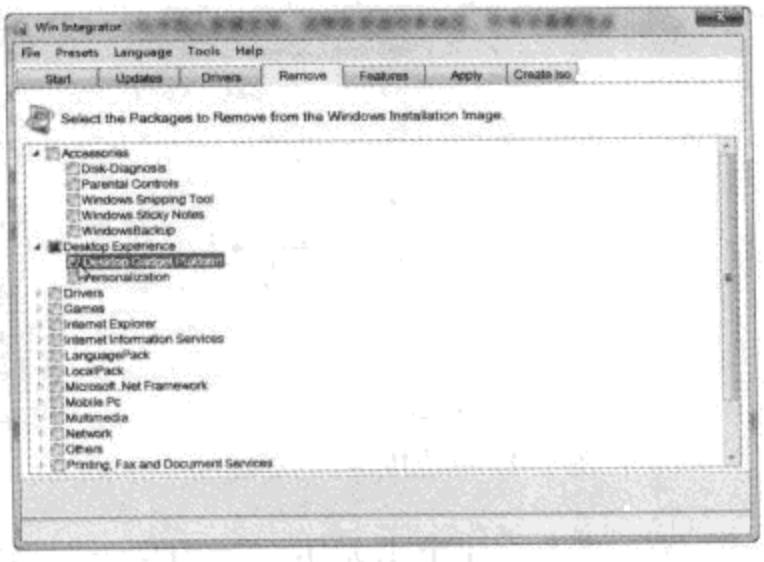


图 1-5　需要慎重增/删的组件

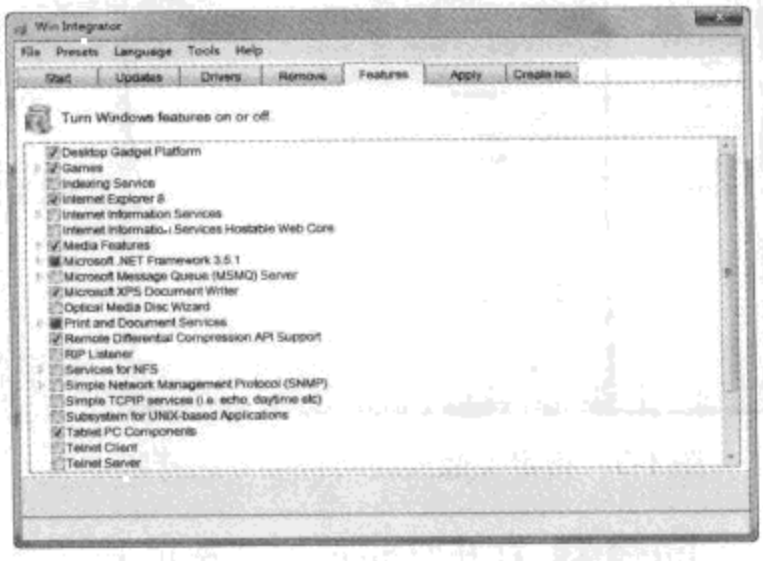


图 1-6　可以放心增/删的组件

到这里，我们已经获得了定制过的 Windows 7 安装文件。Windows 7 的安装方式多种多样，可以通过光盘安装，也可以通过 U 盘，或者直接在 PE 环境下从硬盘安装。但作为最普遍的方法，大部分人可能依然会选择通过光盘安装的方式。因此，对于定制后的 ISO 文件，还需要将其刻录到光盘上。

在刻录光盘时需要注意，ISO 等光盘镜像的刻录与普通文件的刻录不同，必须将其以“光盘镜像”的形式刻录，而不能当做普通文件一样刻录，如果刻录好的光盘中只显示了一个 ISO 文件，这样的光盘既不能用于启动计算机，也不能用于安装 Windows。

如果你的计算机已经运行 Windows 7，则有一种比较简单的办法，在 Windows 7 系统中，用鼠标右键单击创建出的 ISO 文件，指向“打开方式”，并选择“Windows 光盘映象刻录机”，随后即可使用系统内建的功能刻录成光盘。

如果你的计算机没有运行 Windows 7，那么就必须借助第三方光盘刻录软件。很多刻

录机附带的刻录软件通常都具有类似的功能，不过名称可能会有所不同，详细方法请参考刻录软件的说明。

经过上面的操作，我们已经了解了怎样将更新和补丁程序集成到 Windows 的安装文件中。如果不想刻录光盘，或者某些计算机没有光驱，其实还有更简单的方法。只要有容量不低于 4 GB 的 U 盘，并且计算机可以支持从 USB 设备引导（能运行 Windows 7 的计算机通常都可满足该要求），就可以直接使用处理后的 U 盘引导计算机，并完成安装，具体的过程与用光盘安装完全一致。

在将 U 盘连接到计算机后，假设 U 盘的盘符是 E，需要按照下列步骤处理该 U 盘：

STEP 01 打开“开始”菜单，在搜索框中输入“cmd”，在显示的 cmd 程序上单击鼠标右键，选择“以管理员身份运行”，打开管理员命令行窗口。

STEP 02 运行“diskpart”命令，随后运行“list disk”命令，列出本机所有的磁盘（如图 1-7 所示）。

```
C:\Windows\system32>diskpart

Microsoft DiskPart 版本 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
在计算机上: WORKSTATION

DISKPART> list disk

  磁盘 ###  状态           大小     可用     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  磁盘 0    联机             1397 GB  1024 KB
  磁盘 1    联机             1397 GB     0 B   *
  磁盘 2    联机             1397 GB     0 B   *
  磁盘 3    联机             7663 MB     0 B
  磁盘 4    联机               14 GB     0 B

DISKPART>
```

图 1-7　列出所有的本地磁盘

STEP 03 随后需要根据磁盘的大小信息，判断哪个是 U 盘，例如，本例中的 U 盘是“磁盘 4”。接着按顺序执行下列命令，每一行的黑体字是一个完整的命令，“#”符号以及该符号后面的内容是注释，用于解释该命令的作用，不需要输入。

Select disk 4 # 选中 U 盘，这样后续操作都会对 U 盘生效（注意：这里一定要小心，如果错误地选择了其他磁盘，有可能导致数据丢失）。

Clean # 清除该磁盘上的分区表，这样其中的所有分区和数据都将被删除。

Create partition primary # 在该磁盘上使用所有可用的空间新建一个主分区。

Select partition 1 # 选中该主分区，这样后续操作都会对该分区生效。

Active # 将该分区设置为活动的。

Format fs=ntfs quick # 将该分区快速格式化为 NTFS 文件系统。

Assign # 为该分区分配第一个可用盘符。

Exit # 退出 Diskpart 命令行工具。

STEP 04 还是在该命令行窗口中，使用“**cd**”命令进入 Windows 7 安装文件目录（本例中是 d:\Windows），并进入到“boot”子目录下，然后运行“**Bootsect.exe /nt60 X:**”命令

（其中的“X”是给U盘分配的盘符，请根据实际情况替换），该操作会在U盘上复制引导计算机所需的必要文件，如果一切正常，将能看到图1-8所示的界面。

STEP 05 随后将d:\Windows目录下的所有文件和文件夹都复制到该U盘的根目录下。

至此，可用于安装操作系统的U盘制作完成。在使用时，可以和使用光盘安装一样的方法，将U盘连接到USB接口，并通过BIOS或计算机的引导方式选择界面选择使用U盘引导。随后的安装过程和使用传统的U盘安装方法完全相同。

```
D:\Windows\boot>bootsect.exe /nt60 i:
Target volumes will be updated with BOOTMGR compatible bootcode.

I: (\\?\Volume{a611330c-30a8-11df-9c63-001915655aa0})

    Successfully updated NTFS filesystem bootcode.

Bootcode was successfully updated on all targeted volumes.

D:\Windows\boot>_
```

图1-8 将U盘设置为可引导设备

将更新程序整合到Windows安装文件中的方法比较麻烦，因此，有些人可能会纳闷，干嘛非要这样做？安装好系统再进行更新难道不行吗？

如果因为一些原因（例如测试软硬件）需要经常重装操作系统，每次重装完系统之后才安装各种补丁程序，这样很浪费时间。如果需要给多台计算机安装系统，这样不仅浪费时间，还会造成网络带宽的浪费。因此，如果需要面对这些问题，花费一些时间将补丁和更新集成到Windows的安装文件中还是很有必要的。

1.2 安装过程中的注意事项

就算使用集成了最新更新和补丁程序的Windows安装程序安装系统，这也不意味着装好的系统就是安全的，因为在安装过程中，我们还需要注意两个问题：Administrator账户以及网络上的威胁。另外，在安装好Windows 7之后，很多人可能会看到自己的硬盘上被建立了一个100 MB大小的隐藏分区。本节将介绍该分区的用途，以及为什么只有在某些计算机上才能看到该分区。

1.2.1 Administrator账户的问题

Windows 7也是基于Windows NT系统发展起来的，而在所有的Windows NT系统中，在管理员账户方面都有一个最显著的特征：所有的Windows NT系统都自带一个名为Administrator，且对整个系统拥有最高权限的管理员账户。因此，一旦该账户出现问题，例如没有设置密码，或者设置的密码强度不够，就容易导致他人乘虚而入，破坏我们的系统安全。

窍门　为什么不禁用 Administrator 账户

看到这里，可能有人会纳闷：既然 Administrator 账户会带来这么多问题，那为什么不直接将其禁用？毕竟我们还可以使用其他管理员账户。其实这是有原因的，虽然除了 Administrator 账户，系统中还可以创建其他管理员账户，但这些管理员账户和 Administrator 账户有所不同，主要体现在一些特殊情况下。举例来说，如果系统崩溃，已经无法启动，甚至连安全模式都无法进入，这时候可以考虑使用故障恢复控制台。然而只能使用系统自带的 Administrator 账户登录故障恢复控制台，其他管理员账户无法登录。

在安装过程中，这个问题主要体现在对该账户的密码设置方面，下面将介绍这个特殊的账户，同时还会讨论系统自带的 Administrator 账户和其他在安装系统过程中创建的账户。

注意　物理安全很重要。

很多人在系统安全方面存在一个误区，那就是：技术是万能的，靠技术可以解决一切问题。然而在安全领域（以及其他大部分领域）却并非如此。例如，前几年网上曾经盛传过一个所谓的 Windows XP 漏洞，具体内容是："我们都知道，要想在 Windows XP 中进入故障恢复控制台，必须使用 Windows XP 的安装光盘引导计算机，选择修复，同时，如果要修复的是 Windows XP 专业版，还必须使用正确的 Administrator 账户的密码登录才可以使用。如果使用 Windows 2000 安装光盘引导安装了 Windows XP 的计算机，并选择修复，进入故障恢复控制台，无论是 Windows XP 专业版还是家庭版，完全不需要登录，就可以直接进入。"很多人认为这是一个很大的安全漏洞，但微软却一直没有修复这个问题。

在讨论这个问题之前，必须首先明白一个问题：到底什么才是安全的系统？要让自己的系统安全，是否单凭操作系统本身的功能就可以实现？其实上面就是一个很好的例子，虽然这样的"缺陷"可能导致系统不够安全，但严格说来，这种缺陷远非很多人想象的那么严重。因为如果怀有恶意的人可以使用光盘将我们的计算机引导到故障恢复控制台环境下，这也就意味着对方已经可以在物理上接触到这台计算机，而这种情况下，我们还能奢望操作系统的安全功能起什么作用呢？

举一个更形象的例子：如果我是一个黑客，想要攻击某个大型网站的服务器，让服务器的服务中断。为什么我非要费劲寻找成千上万的肉鸡对网站服务器发起拒绝服务（DDoS）攻击？或者为什么要辛苦寻找网站服务器的漏洞？直接把服务器的电源拔掉不就实现目的了吗？不管服务器运行多安全的操作系统，断电后将无法提供任何服务。事实上，重要的服务器一般都放置在保安措施很严密的机房中，同时有很多机制保证服务器在遇到各种突发问题的时候都能继续提供服务，让人拔电源就更不容易了。

因此，在这里也要提醒大家，在按照本书介绍加固操作系统安全的同时，计算机的物理安全问题依然不能忽视。大部分时候，技术都不是万能的。

在 Windows 7 中，Administrator 账户的问题其实很明了，在所有版本的 Windows 7 中，Administrator 账户默认情况下都是被禁用的，而且在安装过程中不需要我们为该账户设置密码。默认的设置下，就算在安全模式中也不能使用 Administrator 账户登录。

另外，有很重要的一点需要注意，虽然将 Administrator 账户启用后，可以在正常模式或者安全模式下使用该账户登录系统，但该账户在默认情况下完全不受用户账户控制功能的限制，有可能带来一定的安全隐患。因此，建议平时使用标准账户或者非 Administrator 的其他管理员账户。关于用户账户控制的相关内容，请参考本书 2.2 节“用户账户控制（UAC）”的相关内容。

1.2.2 来自网络的威胁

在安装过程中，关于网络，只有一个问题需要注意，那就是将系统接入网络的时间。

我们都知道，系统的安装是分阶段进行的，一般情况下，在系统还没有完全安装好的时候，只要网络组件已经安装好，系统就可能已经被接入网络。那么在安装过程中，如果系统已经连通了网络，但其他安全组件尚未启动，就有可能导致隐患。

例如，前几年冲击波病毒肆虐网络的时候，笔者曾亲身经历过的一件事：当时我在给朋友的电脑安装系统，安装的是没有集成任何 Service Pack 的 Windows XP 专业版，安装系统之前忘记了将网线拔掉，而他使用了不需要拨号即可联网的小区宽带。结果在安装系统的过程中，当网络组件被安装好，安装程序还在继续后面的安装时，网络中其他中了冲击波病毒的计算机就对这台计算机发起了攻击，这直接导致系统还没有装完就因为被攻击而自动重启。

对于这个问题上，操作系统本身的一些功能可以有效地避免。例如，在 Windows 7 中，Windows 防火墙是被默认启用的，同时在操作系统的启动过程中，一旦网络组件被成功启动，Windows 防火墙的一部分就会开始生效，限制系统只能进行必要的网络活动，例如，联系 DHCP 服务器获取新的 IP 地址配置。而只有在系统完全启动好，Windows 防火墙组件也全部被成功加载后，系统才可以完整地使用所有的网络功能。

虽然系统自身的一些改进已经让这个问题不再那么突出了，不过为了保险起见，在安装系统的过程中，最好能将网络断开，甚至把网线拔掉，待系统安装好，并配置好防火墙和反病毒软件之后，再将系统连接到网络。

1.2.3 隐藏分区的问题

有些人在安装好 Windows 7，并运行“diskmgmt.msc”打开磁盘管理控制台后可以看到，自己的系统中存在一个 100 MB 的隐藏分区，并且该分区还会被 Windows 标注为“系统”分区（如图 1-9 所示）。但是有些人的系统中并没有这样的分区。这是为什么？为何要创建这样的分区？又如何让安装程序不要创建？

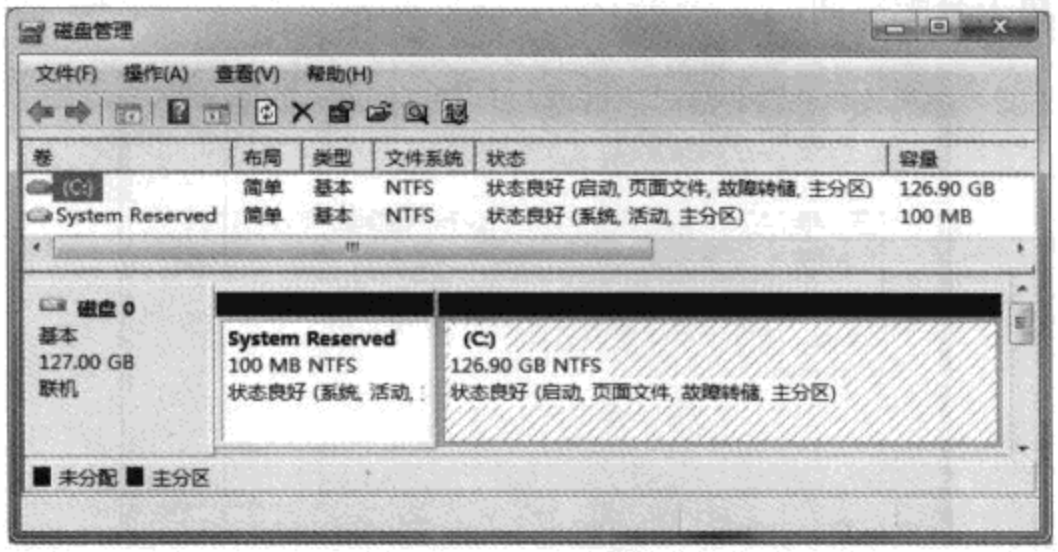


图 1-9　安装程序自动创建的隐藏分区

其实，这个分区中保存了用于启动 Windows 7 系统的所有引导文件，以及 WinRE（Windows 恢复环境）使用的必要文件。如果将其删除，或进行任何操作，都有可能导致 Windows 无法启动。

另外，在使用 BitLocker 功能对本地硬盘分区进行加密的时候，如果要加密系统盘，那么就需要准备一个独立的系统分区（100 MB 大小），用于保存不能被加密的引导文件（有关 BitLocker 功能的详细介绍，请参考本书第 12 章）。在 Windows Vista 时代，如果需要使用这样的功能，往往需要在安装系统之前手工调整硬盘分区，或使用微软提供的一个工具软件。这样做往往很麻烦，而且容易出错。因此，某些情况下，在 Windows 7 中安装程序可以自动创建这样的隐藏分区。

那么什么情况才能创建？其实主要需要满足两个条件：使用介质引导计算机，并进行安装时。这里的介质可以是光盘，或者经过上文介绍的步骤处理过的 U 盘，甚至可以是网络引导。但一定需要使用介质引导计算机，如果是在老版本 Windows 运行的过程中从介质上运行安装程序，是无法创建的。

另外，在安装过程中选择安装位置时，必须选中“未分配”的磁盘空间，而不能选择一个已经创建好的分区。在安装过程中，我们可以看到如图 1-10 所示的界面，在这里可以选择安装 Windows 7 的目标分区。

如果硬盘上已经建立了分区，即使在这里将该分区格式化并安装，安装程序也无法创建隐藏分区。只有选择“未分配空间”，安装程序才能创建两个分区，其中一个是 100 MB 的隐藏分区，用于保存引导文件；另一个则会使用所有剩余的未分配空间，用于保存 Windows 系统文件。

因此，如果是在已经安装有操作系统的计算机上全新安装 Windows 7，并且希望创建这样的隐藏分区，此时可以首选原系统盘（通常是 C 盘），然后单击“驱动器选项（高级）”链接，利用安装程序提供的选项将该分区删除（这里必须要“删除”，而不能“格式化”），

这样即可获得一块未分配空间。

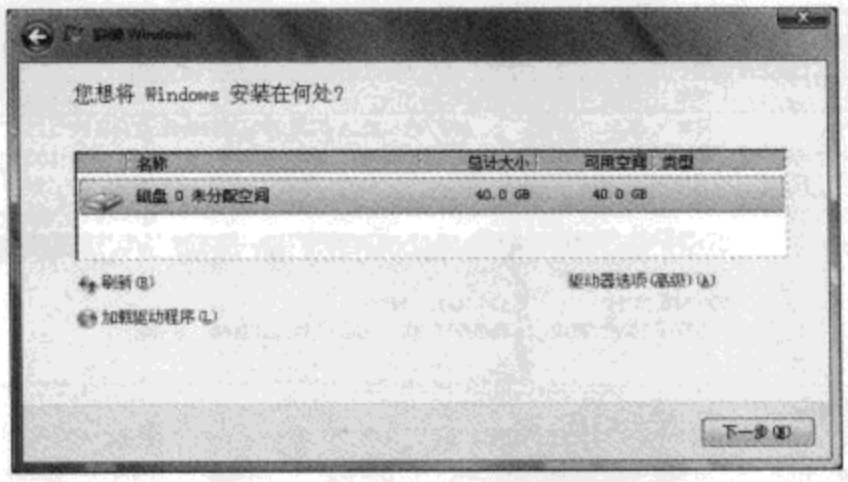


图 1-10　选择系统安装到的分区

1.3　初次使用中的设置

系统安装好之后，第一次启动时，首先会看到一个向导，该向导可以帮助我们设置一些关键的选项，例如，可以创建账户、自定义当前账户的桌面环境、设置时区和网络类别，以及安全保护方式等。

下面以零售版 Windows 7 为例介绍首次运行时需要设置的选项。注意，如果是购买品牌机预装的 OEM 版 Windows，整个过程可能会有所不同，因为品牌机厂商可能会在这个环节中增添一些自定义的选项和内容。

在 Windows 7 下，安装好系统第一次启动的时候，需要在向导中设置很多选项。下面将挑选其中涉及系统安全性的内容进行介绍。

首先是为自己创建账户，以及设置计算机名称的选项。单击“下一步”按钮后，还需要为自己的账户设置密码和密码提示，如图 1-11 所示。

这里需要注意，密码是可选的，如果认为没必要，也可以不输入密码。但因为这里创建的是管理员账户，为了安全起见，最好还是设置一个密码。同时，这里还可以选择是否使用密码提示，通过设置密码提示，如果登录时忘记了密码，Windows 会自动显示这里输入的密码提示，帮助回忆密码。但是要小心，不建议使用密码本身作为密码提示，或者像有些人将类似“我的生日”、“我的手机号码”之类比较容易让人猜测到的密码短语作为密码提示。因为密码提示任何人都可以看到，如果别人打算使用我们的账户登录系统，但不知道密码，如果通过“我的生日”之类的短语猜到我们的密码，那么这个密码就没有意义了。有关密码安全性的信息，请参考下文相关内容；有关密码提示的详细信息，请参考 1.3.2.1 节的相关内容。

接着可以在如图 1-12 所示的界面上设置 Windows 安全选项，只要从提供的选项中根据需要选择即可。

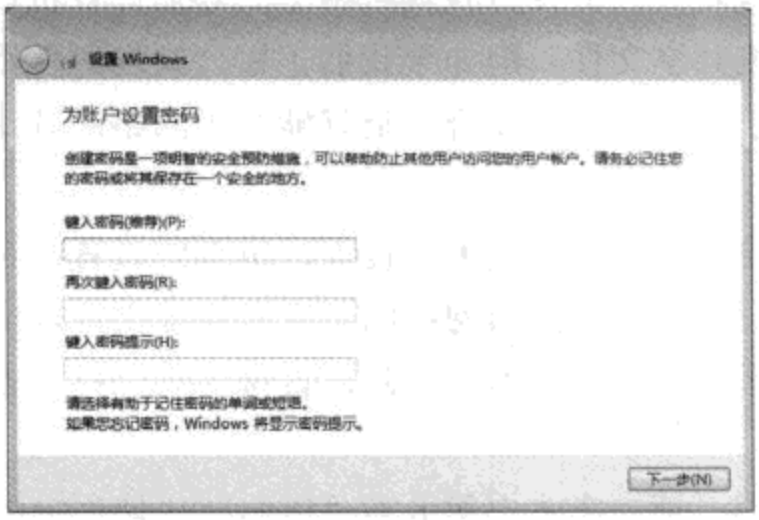


图 1-11　为账户设置密码和密码提示

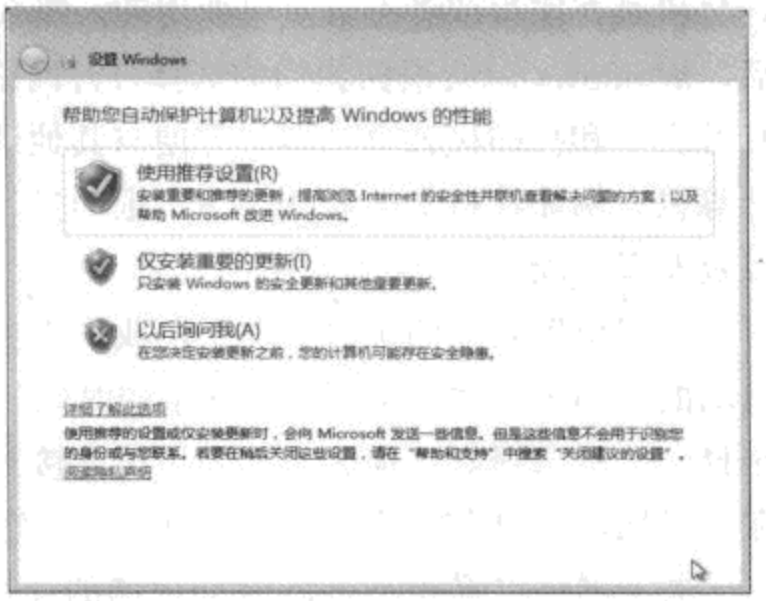


图 1-12　设置 Windows 7 的安全选项

这三个选项之间到底有什么区别？

使用推荐设置　这个选项可以启用 Windows 自动更新、Windows Defender、Windows 问题报告和解决方案，Internet Explorer 仿冒网站筛选等功能的默认设置，并会设置让 Windows 通过 Windows Update 获取有关设备驱动程序的更新，通常建议选择这个选项。

仅安装重要的更新　这个选项只启用 Windows Update 功能，并且只安装关键更新和安全更新，上面提到的其他选项都不会启用。如果没有特殊原因，不建议选择该选项。

以后询问我　如果选择该选项，那么以后每次登录 Windows 的时候都会被询问，直到选择了上面任何一个选项。

如果计算机上安装了网卡，并且在安装 Windows 的过程中已经安装了系统自带的网卡驱动，网卡可以正常工作，那么随后还可以看到如图 1-13 所示的选择网络位置的选项。

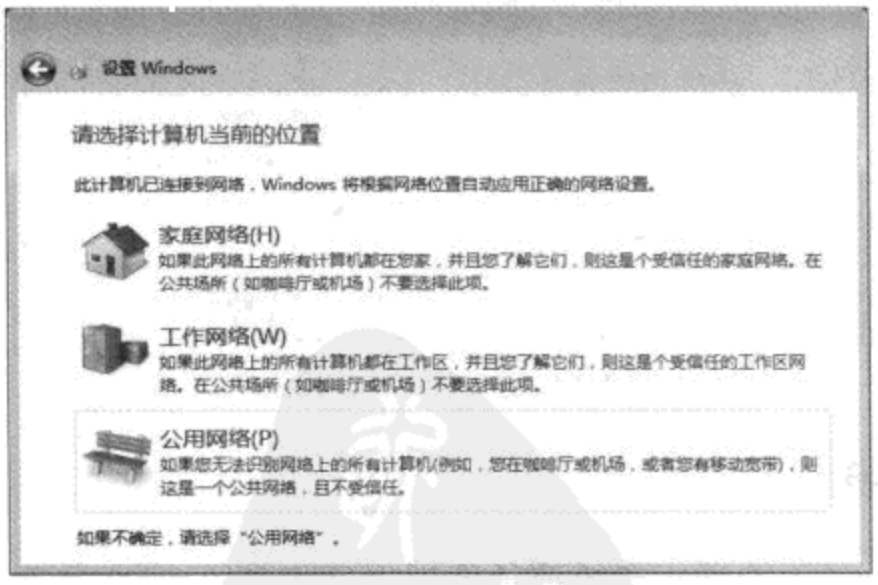


图 1-13　选择恰当的网络位置

网络位置是从 Windows Vista 开始出现的一项功能，简单来说，就是根据网络的实际类型做出适合的配置，这些配置还会被应用给 Windows 自带的防火墙。举例来说，如果这台

计算机是在家里或者办公室里使用的，那么根据实际情况选择“家庭网络”或“工作网络”后，Windows 就会根据我们的选择打开网络发现功能，方便查找局域网上的其他计算机；打开文件和打印机共享功能，方便与其他计算机共享文件。但如果我们正在公共场所使用计算机，例如在机场或者咖啡馆，很明显，为了安全，这种场合下最好能禁用网络的共享以及发现功能。

网络位置功能的优势就在于，我们不再需要根据网络环境手工设置，所有的设置都是自动的。当第一次连接到一个网络的时候，Windows 会询问该网络的位置，并提供选项供选择。一旦选择好，那么下次如果再连接到该网络，系统将不再询问，直接应用同样的设置。当然，如果有需要，我们也可以手工修改。

关于网络位置和 Windows 防火墙的详细内容，请参考本书第 8 章“网络防火墙”中的相关内容。

如果这台计算机位于局域网中，局域网中有其他运行 Windows 7 的计算机，并且创建了家庭组（家庭组是 Windows 7 中新增的共享功能，详细信息请参考本书 7.1.1 节），那么还可以通过输入密码的方式加入该家庭组（如图 1-14 所示），这样就可以直接访问家庭组中所有共享的资源。

如果当前所在局域网中尚未创建家庭组，则可以在这里创建家庭组，并设置密码。

有关家庭组的使用，在这里只简单提及该功能，要了解家庭组的创建和加入、资源的共享和访问，以及退出等更详细的内容，请参考本书第 7 章的相关内容。

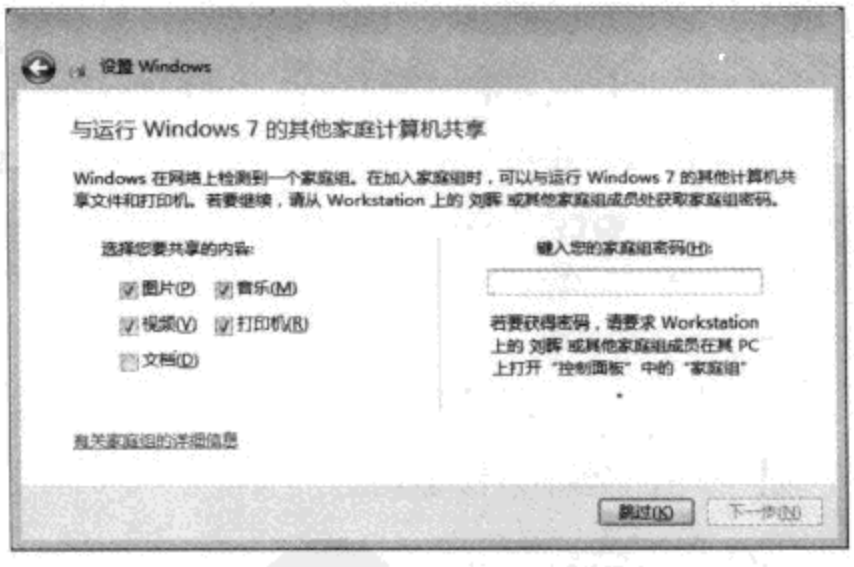


图 1-14　创建或加入家庭组

1.3.1　新建账户并创建密码

所有基于 Windows NT 的操作系统都是多用户操作系统。那么什么是多用户操作系统？这种系统和单用户操作系统相比又有什么优势呢？

我们很多人的计算机都是要和多个人共同使用的，例如，放在家里的计算机，可能每个家庭成员都需要使用。如果是传统的单用户操作系统，那么每个人在使用计算机的时候都只能使用一个公用的账户，这样，一个人对系统更改的设置（例如更换墙纸、屏幕保护，

甚至设置 Internet Explorer 的收藏夹、Cookie 等）都会被其他人直接使用，不仅不方便，还有可能造成隐私泄露。但在多用户操作系统中就简单多了，每个人都可以使用自己的账户和密码（如果有的话）登录。这样一个人对某些选项（主要指针对当前用户的设置，而非针对整个系统的设置）的设置都只能被这个人使用。例如，我们自己设置的墙纸或者 Internet Explorer 收藏夹的内容，别人都看不到。

因此，使用多用户操作系统为每个用户创建一个账户，并使用密码将账户保护起来，这是实现计算机安全的一个很重要的先决条件。

1.3.1.1　账户和账户组的概念

账户是很有用的，那么 Windows 中都有哪些账户，这些账户对系统具有怎样的权限，账户组又是什么意思，这些是本节要介绍的内容。

首先需要明白，在 Windows 中，有两个系统自带的账户：Administrator 和 Guest，其中，前者属于管理员账户，对系统具有完整的控制权限；后者是来宾账户，只能对系统采取最基本的操作，无法修改系统设置。除了这两个账户外，在 Windows 中还有其他一些账户，主要用于一些特殊的环境，例如，用于进行远程协助的账户等，这些账户默认都没有启用，而且一般用户很少需要，因此，这里不再详细介绍。

在 Windows 中，根据权限的不同，基本上有以下三种账户。

- **管理员 Administrator 账户：**就是管理员账户。除此之外，当我们安装好系统第一次启动的时候，在欢迎界面上创建的也都是管理员账户。管理员账户隶属于 Administrator 组，对系统拥有所有的权限，这些权限包括：
  - 创建、更改和删除用户账户和组。
  - 安装和卸载软件。
  - 配置自动更新，或者手工更新系统。
  - 安装 ActiveX 控件。
  - 安装或删除硬件设备驱动。
  - 共享文件夹。
  - 设置权限。
  - 访问所有的文件，包括其他用户的个人文件。
  - 获得文件或文件夹的所有权。
  - 将文件复制或移动到系统目录中。
  - 从备份中还原文件。
  - 给其他用户或者自己分配访问权限。
  - 配置家长控制功能。
  - 配置 Windows 防火墙。
  - 登录系统到安全模式。

- **标准用户：**默认情况下，系统中没有自带标准用户，但我们可以根据实际需要创建标准用户（“标准用户”是 Windows 7 等新版本 Windows 的叫法，在 Windows XP 及之前的版本中，这种账户被叫做“受限账户”）。标准用户隶属于 Users 组，虽然标准用户可以修改绝大部分非关键系统设置，不过却不能修改可能会影响系统安全性或稳定性的设置。标准用户具有的权限包括：
  - 更改自己账户的密码或显示图片。
  - 使用安装在本机的程序。
  - 安装批准的 ActiveX 控件。
  - 配置安全的 WiFi 连接。
  - 查看权限（对于 Windows XP，要求管理员把已经禁用了的简单文件共享）。
  - 在自己的文档文件夹或者共享文档文件夹中创建、更改或删除文件。
  - 还原自己文件的备份。
  - 查看系统时钟和日历。
  - 配置电源选项（仅限 Windows Vista 及以上系统）。
  - 登录到安全模式（仅限 Windows Vista 及以上系统）。
- **来宾用户：**默认情况下，系统中只有一个 Guest 账户属于来宾用户，而且我们没办法直接利用控制面板中的用户账户工具创建其他来宾用户。来宾用户隶属于 Guest 组，拥有与标准用户类似的权限，但受到的限制更多。同时，系统自带的 Guest 账户和其他隶属于 Guests 组的来宾用户的权限也有区别，例如，Guest 账户无法给自己设置密码，但其他来宾用户可以。

除了用户账户，在 Windows 中还有一类安全主体需要注意，那就是账户组。前面我们已经提到过账户组的一些内容，例如管理员账户隶属于管理员组、标准用户隶属于 Users 组、来宾用户隶属于 Guests 组。那么到底什么是账户组，账户组又有什么作用呢？

顾名思义，账户组就是一组用户的集合，简单地说，如果一组用户具有相同的权限，那么就可以创建一个组，将这些用户全部添加到该组中。账户组在企业中使用得比较广泛，例如，如果企业中每个部门所有员工的账户所需要的权限都一样，例如市场部的所有员工都需要一样的权限，而财务部员工则需要一样的权限，那么在为这些人创建账户的时候，最笨的办法就是创建好每个账户后挨个为所有的账户设置权限，这样不仅操作烦琐，而且容易造成遗漏或者错误。这时候就可以使用账户组，例如，为市场部创建一个组，为财务部创建一个组，针对这些组来设置权限，然后将员工按照实际情况添加到不同的组中，这样每个员工也就有了和自己所在组一致的权限设置。这样做不仅方便，而且日后如果员工转换工作岗位，操作起来也很简单，只要把员工从一个组中删除（这里删除的只是用户和账户组之间的对应关系，而非账户），并添加到另一个组就可以了。

Windows 中自带的组有很多，不过一般情况下都很少用到。我们只需要记住最常用的组就行了，这些组是 Administrators 组（注意，名称末尾带有“s”，代表这是一个账户组，

而不是 Administrator 账户）、Users 组，以及 Guest 组。这些组所具有的权限就是上文介绍的管理员账户、标准账户，以及来宾账户相对应的权限。

1.3.1.2　创建账户和账户组

本节将介绍在 Windows 7 下如何创建用户账户和账户组。需要注意的是，如果希望进行这些操作，首先需要使用管理员账户登录 Windows。

1．创建用户账户

在 Windows 7 中，如果希望创建用户账户，可以按照下列步骤操作：

STEP 01　依次单击“开始”→“控制面板”→“添加或删除用户账户”。

STEP 02　单击“创建一个新账户”链接。

STEP 03　在随后出现的页面上输入该账户的名称，并选择希望使用的账户类型。设置好之后单击“创建账户”按钮，即可完成创建。

同样，通过上面的方法只能创建管理员账户或受限账户，虽然大部分情况下都已经够用了，但如果因为某种原因需要创建隶属于其他组的账户，依然需要使用计算机管理控制台中的本地用户和组管理单元。为此，请按照下列步骤操作：

STEP 01　打开“开始”菜单，在搜索框中输入“lusrmgr.msc”并按回车键，打开本地用户和组控制台。

STEP 02　在窗口左侧的控制台树列表中，鼠标右键单击“用户”节点，选择“新用户”，随后可以看到如图 1-15 所示的“新用户”对话框。

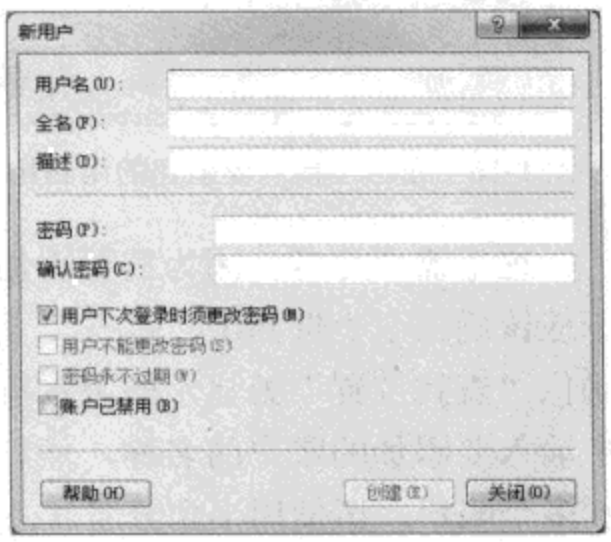


图 1-15　“新用户”对话框

STEP 03　最基本的情况是，只需要输入用户名即可创建账户。如果有必要，还可以输入描述、密码等信息，并通过提供的选项设置账户属性。

STEP 04　设置完毕后单击“创建”按钮，接着单击“关闭”按钮。

按照上述方法创建的账户隶属于“Users”组，属于标准账户，无法执行管理任务。如果需要创建具有管理员权限的账户，则需要调整该账户的隶属关系，具体做法可参考下文。

2．创建和管理账户组

账户组和账户一样，不仅可以创建、删除，还可以对其设置权限。另外，我们还可以编辑组关系，简单地说，就是将新账户加入组，或者将某个账户从组中删除。账户组的所有操作都是在计算机管理控制台的本地用户和组管理单元中进行的。

要想创建账户组，请按照下列步骤操作：

STEP 01　打开“开始”菜单，在“计算机”上单击鼠标右键，选择“管理”，打开计算机管理控制台（也可直接运行“compmgmt.msc”打开）。

STEP 02 在左侧的控制台树中进入到“计算机管理”→“系统工具”→“本地用户和组”→“组”节点。

STEP 03 随后，系统中现有的组都会列在窗口右侧的面板中，双击其中一个组可以打开并调整对应的设置。

STEP 04 如果希望新建组，请用鼠标右键单击“组”节点，打开如图 1-16 所示的“新建组”对话框。

STEP 05 在“组名”和“描述”两个文本框中输入该组的名称和描述，其中的名称是必需的，描述是可选的。接着可以单击“添加”按钮为组添加账户。

STEP 06 单击“添加”按钮后可以看到如图 1-17 所示的“选择用户”对话框。

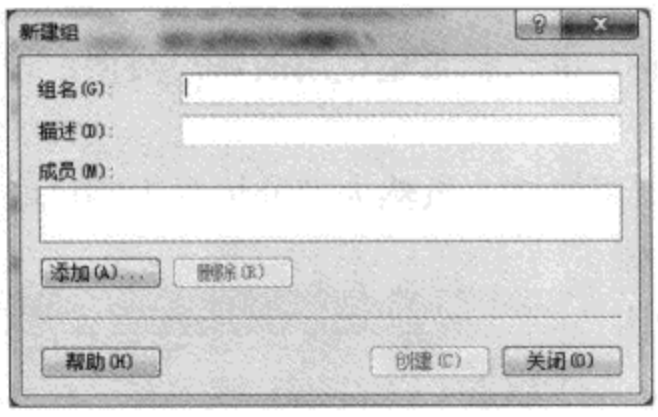


图 1-16　在这里输入要创建的组的相关信息

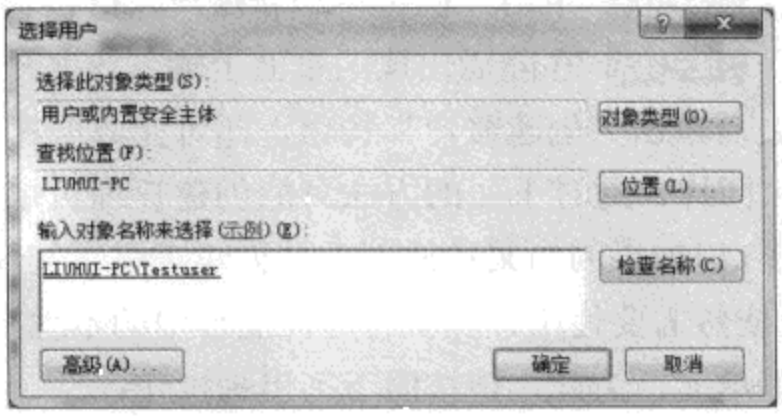


图 1-17　选择要加入该组的账户

这里需要注意，因为需要添加的内容是用户账户，因此，在“选择此对象类型”选项下应该确保至少选择了“用户”，默认设置即可。又因为是针对本机进行的操作，因此，请确保“查找位置”处显示的是本机的名称。接着只需要在“输入对象名称来选择”文本框中输入要添加的账户的名称，然后单击“检查名称”按钮进行确认即可。如果希望一次添加多个账户，请使用半角分号（;）将不同账户隔开。

如果知道要添加的账户的名称，也可以单击“高级”按钮，在随后出现的“选择用户”对话框中单击“立即查找”按钮，这样程序会自动列出所有的本地账户，我们只需要双击目标账户，即可将其添加进来。

STEP 07 将所有希望添加的账户都选中后单击“确定”按钮，即可返回如图 1-16 所示的“新建组”对话框，同时之前选中的账户都会出现在成员列表中。如果希望删除其中的某些成员，只需要将其单击选中，然后单击“删除”按钮即可。

STEP 08 添加了需要的账户后，单击“创建”按钮，这个组就创建好了。

按照上面的方法可以创建账户组，并添加需要的账户到该组中。但日后如果需要调整组关系或者组本身的设置又该怎么办？例如，需要给一个组中添加更多的账户，或者将其中的某个账户删除。这时候只需要在“组”节点下双击目标组，即可看到如图 1-18 所示的“组属性”对话框，并且成员列表中显示了该组的所有账户。

如果需要添加新的账户到该组中，只要单击“添加”按钮，然后像创建组时那样操作，即可将账户添加进来。如果需要删除某个组成员，也只需要将其单击选中，然后单击“删

除”按钮。

我们有时候可能需要进行另一种方式的调整。例如，市场部的员工都位于名为“市场部”的组中，但其中一位员工被调动到财务部工作了，我们需要将他对应的账户在“市场部”组中的关系删除，并将其添加到“财务部”组中。如果同样按照上面的方法操作，难免有些烦琐，这时候我们可以进入“用户”节点，单击该员工的账户，打开属性对话框中的“隶属于”选项卡，如图 1-19 所示。

图 1-18　查看和调整组的成员关系

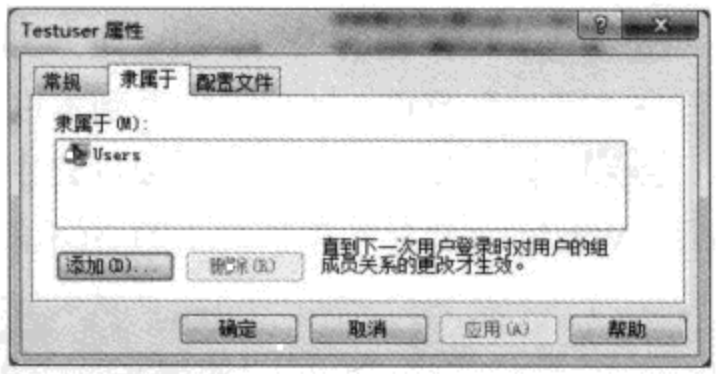


图 1-19　在此可针对具体账户调整组关系

我们只需要在“隶属于”列表中选中希望删除组关系的组，并单击“删除”按钮，然后单击“添加”按钮，选择希望添加到的组即可。

1.3.1.3　设置安全的密码

假设已经按照上文介绍的方法给每个用户创建好了各自的账户，这时候该考虑使用密码保护每个人的账户。

通常，我们在安装好 Windows 后，通过“控制面板”中的“用户账户”工具创建的账户都是无法直接设置密码的，在这种情况下有两种选择：使用计算机管理控制台中的“本地用户和组”管理单元更改其他账户的密码，或者让每个人使用自己的账户登录系统，然后更改密码。

1．使用自己的账户登录后设置密码

如果想要设置自己的账户，也就是说，在账户没有使用密码的情况下加入密码，可按照下列步骤操作：

STEP 01　在使用目标账户登录后，按下“Ctrl+Alt+Del”组合键打开 Windows 安全界面，在这个界面中单击“更改密码”按钮（没错，虽然需要创建密码，不过在这里却要单击“更改密码”按钮），可以看到如图 1-20 所示的界面。

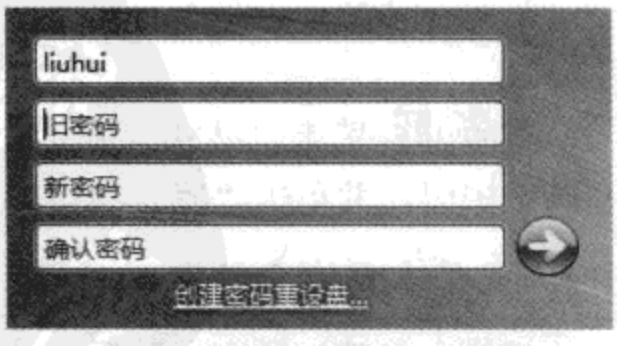


图 1-20　在这里可以创建或更改密码

STEP 02 因为当前没有密码，需要新建密码，所以在“旧密码”一栏留空，并将想要使用的密码输入到“新密码”和“确认密码”这两栏即可。输入完毕后直接按下键盘上的回车键，或者单击“确认密码”一栏右侧的箭头按钮即可。

2. 给其他账户添加密码

除了让每个用户使用自己的账户登录后创建密码外，管理员还可以直接给其他账户（可以是标准用户，也可以是其他管理员用户）创建密码。这个工作可以在“控制面板”的用户账户工具中进行，也可以使用计算机管理控制台的本地用户和组管理单元完成。

STEP 01 打开“开始”菜单，在“计算机”上单击鼠标右键，选择“管理”，打开计算机管理控制台。

STEP 02 在左侧的控制台树中进入到“计算机管理”→“系统工具”→“本地用户和组”→“用户”节点，随后可以看到本机已经创建的所有用户的账户。

STEP 03 用鼠标右键单击想要创建密码的账户，并从右键菜单中选择“设置密码”项，随后，Windows 会显示类似图 1-21 所示的警告信息。

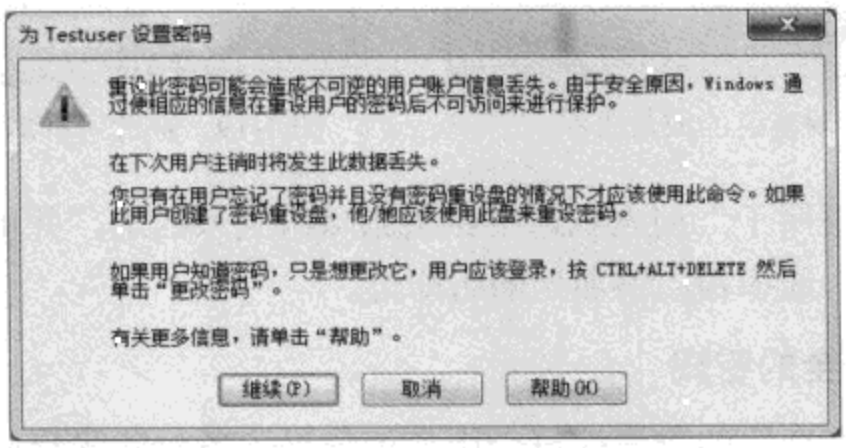


图 1-21　询问是否要给其他账户设置密码

> **注意**　这个警告信息是一项安全措施。在单机和工作组环境中，当我们在 Windows 操作系统中使用管理员账户为其他管理员或非管理员账户创建或修改密码之后，都有可能导致非常严重的后果，例如目标账户的 EFS 加密文件、在 Internet Explorer 浏览器中保存的密码等信息都将无法访问。因此，在进行这个操作的时候一定要谨慎，建议只对新创建的并且还没有登录过的账户这样操作。同时，如果因为该操作导致目标用户原本可以访问的某些文件无法访问，可以将密码重新改回原来的，这样文件将可以恢复访问。

STEP 04 单击“继续”按钮后，可以看到为账户设置密码的窗口，在这里输入新密码和确认密码，并单击“确定”按钮即可。

3. 什么是安全的密码

相信大家都知道密码的重要作用，然而并不是设置了密码就可以保证绝对的安全，因

为有时候，不安全的密码给系统安全造成的影响甚至比完全不使用密码更严重。

如果要创建安全的密码，首先必须保证密码有足够的长度，同时在保证长度的前提下增加密码的组成元素。例如，假设用 26 个小写英文字母组成一个 7 位的密码，那么可能的密码组合就有 26^7 个，而如果用 26 个大小写英文字母（也就是说，一共有 52 个字符）组成一个 7 位的密码，可能的密码组合就有 52^7 个。如果增加长度呢？假设使用 26 个英文字母的大小写形式，一共 52 个字符创建 15 位的密码，那么就有 52^{15} 种不同的组合。可见，随着密码长度和复杂性的增加，可选的密码组合会呈指数趋势增长，进而要破解的难度和所需的时间也会显著增加。

在设置密码之前，这里列出一些关于 Windows 操作系统对密码的要求可供参考。

- 新的 Windows 操作系统（Windows XP/Vista/7）最多可使用长达 127 个字符的密码。
- 密码长度不应少于 8 个字符。
- 密码中不建议使用账户名或者任何与用户个人信息有关的内容。
- 密码中不应该使用完整的可以在字典中查到的单词。
- 密码最好每隔一段时间更换一次，同时新换的密码不应该与旧密码过于相似。
- 密码是大小写敏感的（在 Windows 系统中，密码是唯一大小写敏感的对象）。
- 密码可以由大写英文字母、小写英文字母、数字、特殊符号甚至 ASCII 字符组成。

知道这些规则后，很容易就可以创建出安全的密码，然而在创建密码的时候还需要注意以下问题：

- 密码在保证复杂性的同时还需要易于记忆。
- 永远不要把密码写在纸上，更不要把密码写到贴在显示器边框的记事贴中。
- 不同的场合和用途请尽量使用不同的密码。

如果配合这些建议，要想设置一个既复杂又好记的密码，就不那么容易了，不过还是有好办法。我们可以借助古诗词、格言警句或者自己喜欢的歌词来生成密码，例如，如果要用“不以善小而不为”这句话生成密码，可以首先将其转换为全拼的拼音，每个字的拼音首字母大写，其余字母小写，并在每个字的拼音后面用数字代表音调，这样就得到了“Bu4Yi3Shan4Xiao3Er2Bu4Wei2”一个比较安全的密码，其长度合适，里面包含了大小写英文字母和数字。但我们还可以让这个密码更安全，例如将“Shan”中的字母“S”换成美元符号“$”，将字母“a”换成符号“@”等一些特殊字符。这样的密码不仅好记，而且难以破解，要想通过穷举等方法猜测，那几乎是不可能的。

> **注意**　如果非常关注密码安全问题
>
> 上文中已经讨论过计算机物理安全对整个系统安全性的影响，而在撰写这部分内容时，网络上出现的一则新闻（http://tinyurl.com/ybcmwdo）使得这个问题更值得关注。
>
> 在单机和工作组环境中，Windows 账户的密码都存储在位于本地硬盘上的 SAM

数据库中。在 Windows 正常运行的过程中，SAM 数据库会被锁定，可如果系统被关闭，例如，有人将我们的硬盘连接到其他计算机，或者直接使用一些工具光盘引导计算机，就可以在硬盘上的 Windows 没有运行的情况下，直接读取 SAM 数据库或其他机密信息。虽然账户的密码会被采用不可逆的加密算法加密保存，然而通过暴力穷举，只要有足够的时间，密码的破解一样是可以实现的。

根据网上这篇新闻的介绍，只要有足够快的数据读写速度，一套使用 Athlon X2 4400+处理器的普通家用计算机，搭配一块装满彩虹表（彩虹表可以理解为暴力破解的字典，其中存储了大量可能的字符串组合，而此时的破解就是使用不同的组合挨个尝试，直到找出正确的组合，也就是需要的密码）的 80GB 固态硬盘（固态硬盘可以保证高速读取，进一步降低破解所需的时间），就可以在 5.3 秒时间内破译包括 52 个字母、10 个数字或 33 个特殊字符组成的 14 位 Windows XP 密码。

这样做可以直接看到一个账户的密码，而下文我们还将介绍一些免费的工具，通过这些工具甚至可以在不需要知道原有密码的情况下，直接强制更改某一账户的密码。但这些做法都有一个前提，必须能够在绕过 Windows 安全机制的情况下，用类似“脱机”的形式访问硬盘上的文件。因此，确保系统安全的一个前提就是，一定要保证计算机的物理安全。当然如果有必要，还可以使用本书介绍的 BitLocker 功能将系统盘进一步加密，这样别人就算拿到我们的硬盘，也无法读取其中的数据，更不用说破解我们的账户密码。

1.3.2 忘记密码后的操作

密码是很重要的，我们都应该牢记。然而很多人却经常会忘记密码，这时候也不用慌张，是有办法解决的。

1.3.2.1 密码提示

在任何时候，我们都可以给自己的账户指定一个密码提示，这样在忘记密码后就可以借助密码提示回想密码。但在使用密码提示的时候需要注意，任何人只要能物理上接触到我们的计算机，就能看到密码提示。因此，在选择密码提示的时候尤其需要注意，密码提示必须可以让我们回忆起自己的密码，但又要能保证其他看到的人无法猜测密码。例如，如果用自己的生日作为密码（很多人都这样做），但又使用“我的生日”作为密码提示（很遗憾，依然有很多人这样做），那么别人只要对我们稍微有所了解，密码也就彻底失去作用了。

还是以上文的例子来说吧，如果使用“Bu4Yi3$h@n4Xiao3Er2Bu4Wei2”作为密码，应该怎么设置密码提示？当然可以用“不以善小而不为”作为提示，但有心机的人很容易根据这句话猜测密码，这时候可以使用“要做什么”之类的短语作为提示，这种问题的答案很多，一般陌生人不可能在短时间内猜对。

我们可以在给账户创建密码的同时创建密码提示，或者也可以在创建好密码后只创建

或者修改密码提示。如果在创建密码的同时希望创建密码提示，只要在相应的文本框中输入密码提示就可以了。

如果在创建密码的时候没有设置密码提示，而是希望以后设置，或者在创建了密码提示后希望修改，那么可以按照下列步骤进行：

STEP 01 打开“开始”菜单，依次单击“控制面板”→“用户账户和家庭安全”→“更改 Windows 密码”，随后可以打开当前登录账户的设置页面。

STEP 02 单击“更改密码”链接。

STEP 03 在随后打开的更改密码页面上，在“当前密码”、“新密码”和“确认新密码”文本框中都输入当前使用的密码，然后在“键入密码提示”文本框中输入要使用的密码提示。

STEP 04 单击“更改密码”按钮，这样就可以在不更改现有密码的情况下创建或者更改密码提示。

STEP 05 如果希望在创建密码提示的同时更改密码，则可以在“当前密码”文本框中输入现在正在使用的密码，然后在“新密码”和“确认新密码”文本框中输入新的密码。

在设置好密码提示后又忘记了密码的情况下，就可以使用密码提示帮助自己回忆密码。

对于 Windows 7，在欢迎屏幕上默认并不会显示密码提示，也不提供能够打开密码提示的按钮。只有当使用错误的密码尝试登录并失败后，Windows 才会报告密码错误，单击“确定”按钮后会回到欢迎屏幕，这时候密码提示就会直接显示在密码框的下方，如图 1-22 所示。

图 1-22　欢迎屏幕上显示的密码提示

1.3.2.2　密码重设盘

在忘记密码之前，还可以随时给自己的账户创建一张密码重设盘，这样日后就算忘记了密码，只要提供密码重设盘就可以重置密码。同时这张盘的好处在于，就算在创建密码重设盘之后自己修改了密码，在提供了重设盘之后依然可以重设密码。

在老版本 Windows 中就提供了创建密码重设盘的功能，不过当时只能使用传统的 3.5 寸软盘作为密码重设盘，而现在依然配置软驱的计算机已经很少了，因此，在 Windows 7 中，除了最传统的软盘，还可以使用 U 盘或者光盘，这样更加方便。

要创建密码重设盘，请按照下列步骤操作：

STEP 01 打开“开始”菜单，依次单击“控制面板”→“用户账户和家庭安全”→“更改 Windows 密码”，随后单击窗口左侧任务列表中的“创建密码重设盘”链接，打开忘记密码向导。

STEP 02 在向导的第二个页面中，列出了本机所有的可移动存储设备，例如软驱、U 盘或者光盘刻录机。因此，如果想要使用软驱，请事先插入软盘；如果希望使用 U 盘或移动硬盘，请事先将其与计算机连接；如果想要使用光盘，请事先将空白光盘放入光驱。选

择好想要使用的设备后，单击“下一步”按钮。

STEP 03 输入当前账户的密码，继续单击“下一步”按钮。

STEP 04 稍等片刻，密码重设盘就创建好了。

如果日后忘记了自己的登录密码，那么在欢迎屏幕上输入了错误的密码后，Windows会在密码输入框下方显示一个“重设密码”按钮，单击它后可以打开重置密码向导。在向导中选择密码重设盘的来源，经验证无误后，输入新的密码和密码提示即可。

在使用密码重设盘时有一些问题需要注意：密码重设盘实际上真正生效的是其中保存的一个密钥文件。因此，完全可以将这个密钥文件复制并保存到不同的位置。但正因为如此，这个文件的安全性就非常重要，任何人只要获得这个文件，都可以重设我们的 Windows 账户密码。因此，对于充当密码重设盘的设备（例如 U 盘或移动硬盘），建议不要用于其他操作，以免被盗用。

另外，密码重设盘并不影响受修改密码操作的影响。也就是说，在创建密码重设盘后，如果修改了账户密码，那么并不需要重建重设盘，使用原来创建的重设盘依然可重设修改后的密码。

1.3.2.3 其他破解工具

对于计算机用户来说，最头疼的情况是没有创建过密码提示或者密码重设盘，或者虽然创建了，但是因为各种原因没能生效。这时候难道只能重装系统？其实这时候可以考虑使用其他工具，这类工具通常都是可引导介质，例如光盘或者软盘，用这些介质引导计算机后可以进入其他操作系统（DOS 或者 Linux）下，在这些操作系统中直接对 Windows 的 SAM（里面保存了所有本地账户的安全信息）文件进行破解，即可查看系统中每个账户的密码，或者在不知道密码的情况下修改密码（这类工具软件很多，功能各有差别，但基本都可以用于重设或者查看忘记的密码）。

还有一个问题需要注意：对于 Windows 2000 操作系统，如果能在操作系统没有运行的情况下删除 Windows 2000 的 SAM 文件，那么账户的密码将会被清空。这个方法只能用于 Windows 2000，然而网上有很多不负责任的文章说该方法可以用于 Windows XP/Vista/7 等较新的系统，很多人照做后导致系统崩溃。请一定要记住，删除 SAM 文件的方法对 Windows XP 以后的系统都无效。

这类工具有很多，其中有些是售价昂贵的商业软件，但也有可以免费使用的软件。为了节约成本，本书会介绍一个叫做 Offline NT Password & Registry Editor（下文统一简称为 Editor）的免费软件，该软件可以在不知道当前密码的情况下脱机重设单机或工作组环境下 Windows 操作系统本地用户账户的密码，可支持单机和工作组环境下 32 位以及 64 位的 Windows XP/Vista/7/2003/2008 等系统。该软件的下载地址是：http://tinyurl.com/ycgj7qh。

注意 这并不算是安全漏洞

有人会问了，如果随随便便用一个软件就可以重设 Windows 账户的密码，那

Windows 还有什么安全性可言。其实这要从 Windows 保存本地账户的登录信息的方式，以及这类软件的工作原理说起。首先要明白一个问题，这类软件通常只能用于单机或者工作组环境下的 Windows 操作系统，因为在这样的环境下，Windows 中只有本地用户账户，同时账户的名称以及登录密码等信息都保存在一个叫做 SAM（Security Account Manager，安全账户管理器）的文件中，该文件位于 %SystemRoot%\system32\config 文件夹下。当我们登录的时候，Winlogon 进程首先会获取我们在欢迎屏幕或者“Windows 登录”对话框中提供的用户名和密码，并将获得的信息和 SAM 数据库中保存的记录进行对比。如果能够找到匹配的项目，则证明该用户名和密码是有效的，可以继续进行登录；如果找不到匹配的项目，用户就会被拒绝登录。

所有这类可以查看或者重设 Windows 账户密码的软件实际上都是在破解 SAM 文件。在 Windows 运行的情况下，SAM 文件通常会被操作系统锁定，无法直接读取或者复制，然而通过很多方法可以绕过这一限制，例如，将硬盘连接到其他计算机上直接读取，或者使用引导光盘将计算机引导到特殊的 DOS 或者 Linux 环境下读取。而一旦可以读取到 SAM 文件，虽然 SAM 文件中的信息是被加密的，但理论上，任何加密方法都可能被破解，只不过区别在于破解所需的时间。

要避免这种危险其实也很简单，首先，一定要保证重要计算机的物理安全。相信大家都已经知道，要破解 SAM 文件，必须在操作系统没有运行的情况下进行，这叫做脱机攻击。例如破解者必须能够拿到计算机的硬盘，或者使用具有引导功能的软盘或光盘引导计算机。只要能够有效地保证计算机的物理安全，这类程序在很大程度上都将失效。

另外，在条件允许的情况下请尽量使用长密码。因为根据计算，密码长度增加，破解的难度和所需时间将会呈指数方式增长。同时配合长密码，我们还需要按照实际情况频繁更换密码。例如，假设当前使用的密码复杂程度决定了要破解该密码需要长时间的运算（假设需要 40 天），而我们每 30 天就更换一次密码。这样破解者就算能够计算出密码，等计算出来后，我们的密码早已经更换了。因此，可以通过组策略限制 Windows 对密码的加密方式，以及通过其他密码策略增强系统安全性，相关内容请参考本书 3.1 节“账户策略”的内容。

对于 Windows 7 企业版和旗舰版，其中包含的 BitLocker 功能也可以有效地防范对操作系统的脱机攻击。有关 BitLocker 的详细信息，请参考本书第 12 章的相关内容。对于不包含 BitLocker 功能的 Windows 7 版本，则可以使用系统自带的 Syskey 程序。详细信息请参考本书 1.3.4.2 节“Syskey”的相关内容。

需要注意的是，对于域环境中的 Windows 系统，这类软件往往也只能针对本地账户生效，而无法对域账户生效。因为域账户的登录信息都是保存在域控制器上的，因此，域环境在这方面的安全性要更高一些。

虽然简单介绍了如何防范对操作系统的脱机攻击，不过有时候我们可能依然需要进行这种操作。例如，公司员工离职前忘了将自己的账户密码告诉同事，或者忘记了自己家里计算机的登录密码。需要提醒大家注意的是，这类软件很容易获得，而且使用方法也很简单，但随意对他人的计算机进行攻击或者盗用可能会触犯法律。

首先访问 Editor 的网站，并单击网页顶部的“Bootdisk”按钮，在随后的页面上拖动网页，在网页中部找到“Download”栏目，这里列出了所有可供下载的链接。因为 Editor 可以使用多种介质引导计算机，例如软盘、光盘或者 U 盘，因此，首先需要按照想要使用的介质下载对应的版本，例如，如果希望使用光盘引导计算机（不建议使用软盘版本，因为根据网站上的说明，软盘版本可能会让 Windows 崩溃），可以选择标记为“Bootable CD image”的文件来下载，文件大小在 3 MB 左右。在写本书的时候，Editor 的更新日期是 2008 年 8 月 2 日。

在使用该软件之前，有一些问题需要注意：

- 该软件可以用于单机或工作组环境下的所有 Windows NT/2000/XP/2003/Vista/7 系统，同时可以用于 64 位 Windows 系统。
- 如果希望重设 Windows 中某个账户的密码，而该账户有 EFS 加密文件，那么重设密码后，所有的 EFS 加密文件都将无法读取和解密。
- 对于光盘版本，下载回来的文件解压缩后可以得到一个.iso 文件，请直接使用光盘刻录软件将该文件以**光盘镜像**的形式刻录到 CD 刻录盘上。注意，一定要以光盘镜像的形式进行刻录，而不能像普通文件那样刻录，否则刻录的光盘将无法引导计算机。对于 Windows 7，本身就可以将 ISO 文件以光盘镜像的形式刻录，为此只需要在解压缩出来的 ISO 文件上单击鼠标右键，指向“打开方式”，选择“Windows 光盘映象刻录机”即可。

准备好这样一张光盘后就可以开始了，下面将以破解 64 位 Windows 7 的账户密码为例进行介绍。

STEP 01 将刻录好的光盘放入光驱中，然后重启计算机，并让计算机从光驱引导（可能需要调整 BIOS 设置，具体方法请参考计算机或主板的说明书）。

STEP 02 光盘引导计算机后，首先会显示一些引导选项，例如，是否启用 USB 设备，以及显示参数设置等。通常情况下使用默认选项即可，因此，可以直接按下回车键，开始进行引导，这将会把计算机引导到一个运行在光盘上的 Linux 环境下。

STEP 03 看到图 1-23 所示的界面后，就表示系统已经引导成功了。

STEP 04 注意屏幕底部，如果计算机中安装了多块硬盘，程序首先会让我们选择操作系统所在的硬盘。但如果计算机上只安装了一块硬盘，就会跳过这一步，然后要求我们选择安装了操作系统的分区，或者使用下列选项：

q：退出。

d：自动加载硬盘。

m：手工加载要使用的硬盘。

f：从软驱/USB 设备获取所需的磁盘控制器驱动。

a：显示找到的所有分区。

l：只显示符合条件的 Windows（NTFS）分区。

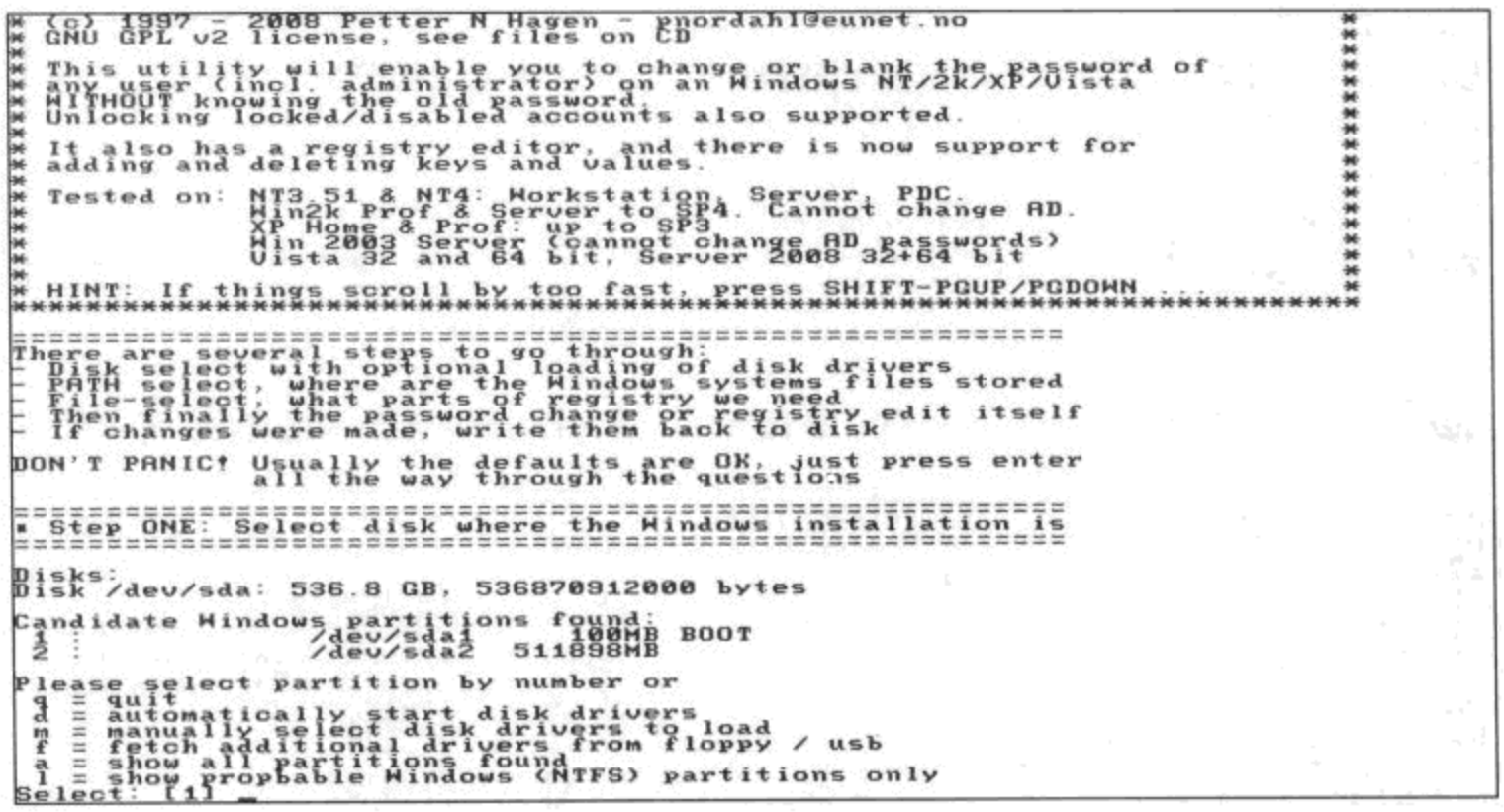


图 1-23　用光盘成功引导后显示的界面

让我们回头再看看程序提示的信息，首先注意在屏幕底部有这样一行内容：

```
Disks:
Disk /dev/sda: 536.8 GB
```

这一行显示了当前选中的硬盘位置以及容量。在这一行下方的内容是：

```
Candidate Windows partition found:
1:     /dev/sda1   100MB Boot
2:     /dev/sda2   511898MB
```

表示在 Disk /dev/sda 这块硬盘上找到了两个可能的 Windows 分区（一个 100 MB 的隐藏分区，一个包含 Windows 系统文件的分区，此时需要处理的是包含 Windows 系统文件的分区，也就是 sda2）。因此，需要输入“2”并按回车键。

如果这里没有列出任何硬盘，那么请输入“d”或“m”并按回车键，重新加载硬盘。如果硬盘已经加载，但没有显示任何分区，可能是因为光盘上的 Linux 系统没有所需的存储子系统驱动，例如可能使用了 RAID 或 SCSI 控制器，或者一些比较罕见的 SATA 控制器。其实则需要输入“m”，并通过软盘或 USB 存储设备提供所需的 Linux 驱动程序，然后输入“a”刷新。

STEP 05 输入目标分区并按回车键后，可以看到如图 1-24 所示的界面（为了节省版面，

下文只截取屏幕中新增加的或者变化了的内容）。

接下来需要选择 SAM 文件的保存位置。通常，如果选择默认安装方式，直接按下回车键即可。如果 SAM 文件在其他位置（例如，Windows 使用了自定义的安装目录），请手工输入，并按下回车键。

```
Selected 2

Mounting from /dev/sda2, with assumed filesystem type NTFS
So, let's really check if it is NTFS?

Yes, read-write seems OK,
Mounting it. This may take up to a few minutes:

Success!

================================================================
* Step TWO: Select PATH and registry files
================================================================
What is the path to the registry directory? (relative to windows disk)
[Windows/system32/config] : _
```

图 1-24　选中分区后的显示结果

STEP 06 指定好 SAM 文件的位置，并按下回车键后，可以看到如图 1-25 所示的界面。

```
================================================================
* Step TWO: Select PATH and registry files
================================================================
What is the path to the registry directory? (relative to windows disk)
[Windows/system32/config]
EXPAND Windows/System32/config
-rwxrwxrwx     2 0          0           28672 Nov  1 13:26 BCD-Template
-rwxrwxrwx     2 0          0        29097984 Mar 16 09:22 COMPONENTS
-rwxrwxrwx     2 0          0           65536 Mar 16 09:22 COMPONENTS{016888b9-6c6f
-11de-8d1d-001e0bcde3ec}.TM.blf
-rwxrwxrwx     2 0          0          524288 Mar 16 09:22 COMPONENTS{016888b9-6c6f
-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
-rwxrwxrwx     2 0          0          524288 Jul 14  2009 COMPONENTS{016888b9-6c6f
-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
-rwxrwxrwx     1 0          0          262144 Mar 16 09:22 DEFAULT
drwxrwxrwx     1 0          0               0 Jul 14  2009 Journal
drwxrwxrwx     1 0          0            4096 Nov  1 14:28 RegBack
-rwxrwxrwx     1 0          0          262144 Mar 16 09:22 SAM
-rwxrwxrwx     1 0          0          262144 Mar 16 09:22 SECURITY
-rwxrwxrwx     1 0          0        39583744 Mar 16 09:22 SOFTWARE
-rwxrwxrwx     1 0          0        11534336 Mar 16 09:22 SYSTEM
drwxrwxrwx     1 0          0            4096 Nov  1 13:30 TxR
drwxrwxrwx     1 0          0            4096 Nov  1 13:27 systemprofile

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] : _
```

图 1-25　指定 SAM 文件的位置后看到的结果

在这里需要指定要加载的注册表内容，通常，如果需要重设账户密码，只要使用默认的设置“1”，然后按下回车键即可。

STEP 07 随后可以看到如图 1-26 所示的界面。因为需要重设账户的密码，因此，可以使用默认的选项“1”，然后按下回车键。

STEP 08 接下来，Editor 会列出系统中所有的本地账户，如图 1-27 所示，我们可以根据实际需要选择其中的某个账户。例如，该程序默认会选中 Administrator 账户，如果希望重设该账户的密码，可以直接按下回车键，或者可以直接输入其他想要重设密码的账户的名称，然后按下回车键。

STEP 09 随后可以按照需要输入新的密码，并确定。这里有个问题需要注意：输入的密码会在屏幕上明文显示，而且不需要再次输入确认。因此，设置密码的时候请小心，不要输入错误。不过，如果输错了也没关系，用这个软件修改密码也是非常简单的。

另外，输入新的密码，并按下回车键后，输入“y”，并按回车键，即可确认更改。

```
================================================================
* Step THREE: Password or registry edit
================================================================
chntpw version 0.99.6 080526 (sixtyfour), (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0x7000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 291/21976 blocks/bytes, unused: 4/2408 blocks/bytes.

Hive <SYSTEM> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
Page at 0xac8000 is not 'hbin', assuming file contains garbage at end
File size 11534336 [b00000] bytes, containing 2552 pages (+ 1 headerpage)
Used for data: 179774/11071384 blocks/bytes, unused: 5625/147816 blocks/bytes.

Hive <SECURITY> name (from header): <emRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0x6000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 389/19856 blocks/bytes, unused: 7/464 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length        : 0
Password history count         : 0

<>=========<> chntpw Main Interactive Menu <>=========<>

Loaded hives: <SAM> <SYSTEM> <SECURITY>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
  - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> _
```

图 1-26　SAM 文件中提供的内容和可进行的操作

```
===== chntpw Edit User Info & Passwords ====

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  | dis/lock |
| 01f5 | Guest                          |        | dis/lock |
| 03ea | HomeGroupUser$                 |        |          |
| 03e9 | liuhui                         | ADMIN  |          |
| 03eb | Testuser                       |        | *BLANK*  |

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] _
```

图 1-27　可重设密码的账户

至此，密码的修改已经完成了。不过为了使设置生效，还必须按照正常途径退出程序，否则，所有的修改将无法保存。

在图 1-28 所示的界面上确认了修改后，输入“!”并按下回车键，然后输入“q”并再次按下回车键。最后程序会询问是否保存修改，并且默认为“否”，因此，输入“y”并按回车键。现在把光盘取出来，然后重新启动计算机，在不需要密码的情况下，用之前处理过的账户即可成功登录。

```
RID     : 1001 [03e9]
Username: liuhui
fullname:
comment :
homedir :

User is member of 1 groups:
00000220 = Administrators (which has 2 members)

Account bits: 0x0214 =
[ ] Disabled        | [ ] Homedir req.      | [X] Passwd not req.  |
[ ] Temp. duplicate | [X] Normal account    | [ ] NMS account      |
[ ] Domain trust ac | [ ] Wks trust act.    | [ ] Srv trust act    |
[X] Pwd don't expir | [ ] Auto lockout      | [ ] (unknown 0x08)   |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)    | [ ] (unknown 0x40)   |

Failed login count: 0, while max tries is: 0
Total  login count: 10

- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
(4 - Unlock and enable user account) [seems unlocked already]
 q - Quit editing user, back to user select
Select: [q] > _
```

图 1-28　清空所选账户的密码

因为该程序本身的不足，有时候可能看似已经修改了账户的密码，但使用新密码依然

无法登录，这时候可以试试看将该账户的密码清空（在图 1-28 所示的界面上直接按下“1”，然后回车），使用空密码登录，然后创建密码。同时要注意，如果是破解 Windows Vista 及以上系统的密码，一定要直接将密码设置为空白，而不是修改为其他密码，只有这样才可以成功。

除了重设账户密码，Offline NT Password & Registry Editor 还有很多其他功能，限于篇幅，本书不再过多地介绍，感兴趣的朋友可以自己研究。

1.3.3 管理其他账户

上文已经说过，基于 NT 的 Windows 系统都是多用户操作系统，它可以让每个用户在自己的账户下对一些非关键系统选项进行自定义设置。当然，每个用户可以修改哪些设置取决于该用户所在的用户组，准确地说，取决于该用户具有的权限。

只要有足够的权限，用户就可以修改绝大多数系统设置，包括管理其他用户的账户或者账户环境。这是本节将要介绍的内容。

1.3.3.1 重设其他账户的密码

如果忘了自己账户的登录密码，并且使用密码提示也无法想起，同时也没有制作密码重设盘，那么在考虑使用其他软件进行脱机破解之前，先看看系统中有没有其他管理员账户。如果有，可使用这些账户登录系统，然后重设账户密码即可。

在重设他人账户密码之前需要记住，这样做会导致对方账户的 EFS 加密文件、网页上保存的密码等机密信息无法访问。因此，如果不是万不得已，通常不建议使用这种方法。

使用管理员账户登录 Windows，然后就可以在控制面板的用户账户工具中进行重设。

STEP 01 打开“开始”菜单，在“计算机”上单击鼠标右键，选择“管理”，打开计算机管理控制台。

STEP 02 在控制台窗口左侧的控制台树中依次展开“系统工具”→“本地用户和组”→“用户”。

STEP 03 在右侧面板中用鼠标右键单击要修改密码的账户，从右键菜单中选择“设置密码”。

STEP 04 随后，系统会显示一个“警告”对话框，提醒我们更改其他账户的密码有可能产生的后果。

STEP 05 仔细阅读说明，如果可以接受该后果，单击“继续”按钮。

STEP 06 在随后出现的“设置密码”对话框相应的文本框中输入新的密码，然后单击“确定”按钮。

这样，该账户就可以使用新密码登录了。

1.3.3.2 设置其他账户的环境

有时候，我们可能会希望实现这样的目的：使用这台计算机的人使用自己的账号登录

后，可以在“开始”菜单或者桌面上看到某个程序的快捷方式，或者在 Internet Explorer 的收藏夹中看到某些同样内容的收藏。应该怎样实现这个目的呢？

每个账户各自的设置（例如，“开始”菜单快捷方式或者 Internet Explorer 收藏内容）都是保存在该账户对应的配置文件夹中的。因此，每个账户登录后对这些内容的修改实际上修改的是自己的配置文件，这样做并不会影响本机上的其他账户。

那么配置文件到底在哪里？首先需要明确一点：大部分关键的配置文件夹都具有隐藏属性，默认情况下，Windows 的资源管理器并不显示这些文件夹，因此，必须先设置资源管理器显示隐藏文件，操作步骤如下：

STEP 01 打开“计算机”窗口，按下键盘上的“Alt”键，这样资源管理器窗口会显示出菜单栏。

STEP 02 在菜单栏上依次单击“工具”→“文件夹选项”→“查看”，打开“文件夹选项”对话框的查看选项卡。

STEP 03 在“高级设置”列表中，取消对“隐藏受保护的操作系统文件（推荐）”选项的选择，并在随后出现的“警告”对话框中单击“是”按钮。

STEP 04 选中“显示隐藏的文件和文件夹”选项。

经过这样的设置，Windows 资源管理器就可以显示硬盘上的所有文件和文件夹了。注意，有很多关键的系统文件是隐藏的，而经过上述设置后，这些文件都将显示在资源管理器窗口中。因此，如果看见陌生文件，而不确定这个文件是做什么用的，最好不要对文件进行任何操作（例如修改或删除），以免影响系统或其他程序的正常运行。

在 Windows 7 下，用户的配置文件夹是系统盘根目录下的“用户”文件夹，打开该文件夹后可以看到系统中每个本地账户对应的配置文件，双击代表不同用户账户的文件夹后，可以看到每个配置文件中保存了有关该账户所有的自定义设置内容，如图 1-29 所示。

图 1-29　Windows 7 下的用户配置文件

首先应该注意到，在 Windows 7 的用户配置文件夹下有一些文件夹带有箭头图标。熟

悉 Windows 的人应该知道，这个图标代表了快捷方式。也就是说，这些文件夹并不存在，只是快捷方式，这又是为什么？

在 Windows 7 中，用户配置文件方面发生了一些小变化，那就是取消了以往一些约定俗成的路径，或者将某些路径保存在新的位置下。然而为了照顾老程序的兼容性，因为一些老的应用程序可能需要向这些目录写入内容，此时，Windows 7 的虚拟重定向功能就会自动将数据写入其他目录；同时，一旦这些软件在运行过程中需要从这两个文件夹中读取文件，虚拟重定向功能也会将文件读取请求定向到其他位置。关于虚拟重定向的详细内容，请参考本书 2.3 节“文件和注册表虚拟化”的相关内容。

窍门　快速打开自己的配置文件夹

在 Windows 7 下，如果希望用最快的方法打开自己的配置文件夹，只要打开“开始”菜单，然后单击“开始”菜单右上角自己的用户名即可。

让我们用一个简单的例子进行介绍。假设需要本机所有的本地账户在登录后都可以在桌面上看到某个程序的快捷方式，可以这样操作：

STEP 01 使用管理员账户登录，在桌面“开始”菜单或 Windows 资源管理器中找到该程序的快捷方式，单击鼠标右键，选择“复制”。

STEP 02 打开“计算机”窗口，进入到系统盘根目录下，然后依次进入“用户”→“公用”→“用户桌面”文件夹（该文件夹的实际路径是 users\public\desktop，只不过 Windows 资源管理器将其翻译成了更“友好”的名称。另外，“桌面”文件夹具有隐藏属性，需要按照上文的方法设置显示隐藏文件后才可以看见）。

STEP 03 用鼠标右键单击文件夹内的空白处，选择“粘贴”，将之前复制的快捷方式粘贴到这里。

经过上述处理，所有登录到本机的本地账户的桌面上都将会出现我们粘贴的这个程序的快捷方式。

窍门　“开始”菜单内容在哪里

在 Windows XP 中，每个账户的配置文件夹下都有一个名为“开始菜单”的文件夹，在这里可以自定义每个用户的开始菜单内容。但在 Windows 7 下会发现，每个账户的配置文件夹里确实有一个“开始菜单”，那只是快捷方式，而且双击后无法访问。通过阅读上文我们应该已经知道了，这是虚拟重定向功能在起作用，那么，Windows 7 的开始菜单内容被重定向到哪里了？很简单，首先打开“开始”菜单，并在“所有程序”上单击鼠标右键，选择“打开”，这样即可打开当前用户的“开始菜单”文件夹；如果选择“打开所有用户”，则可以打开“公用”账户的“开始菜单”文件夹。因此，在 Windows 7 中，我们可以在这些地方自定义自己或者他人的开始菜单内容。

窍门　为什么有些快捷方式好删除，有些不好删除

很多人可能已经发现了，当我们试图删除开始菜单或者桌面上的快捷方式时，会遇到两种截然不同的情况。使用同一个账户登录，在删除自己桌面或开始菜单上的快捷方式时，有些快捷方式很容易就可以删除，但有些则需要进行确认或者输入管理员账户的密码，这是为什么？其实通过本节的阅读就很好理解了，这两种不同的现象取决于快捷方式的保存位置，如果要删除的快捷方式保存在当前用户的配置文件中，那么直接删除即可；如果要删除的快捷方式保存在“公用”配置文件中，因为我们的删除会影响到其他用户，因此，需要有管理员权限。至于快捷方式保存在哪个配置文件夹中，这取决于该程序的安装程序的设置。

1.3.3.3　管理配置文件

在配置文件的管理方面，本书只介绍其中一个比较有用的功能，同时还有一个需要注意的问题。

有时候因为各种原因，损坏的配置文件可能会导致某个用户使用计算机或者其他软件的时候遇到异常。通常情况下，如果同一台计算机上只有某个用户遇到某个问题，而其他用户登录后没有这种问题，那么就可以判断该问题和用户的配置文件有关系，可能是文件损坏或者配置错误导致的，这时候可以用默认配置文件覆盖该用户自己的配置文件，具体方法如下：

STEP 01　将该用户的账户注销，使用管理员账户登录。在“计算机”上单击鼠标右键，选择“属性”，打开系统属性窗口。

STEP 02　单击窗口左侧“任务”列表中的“高级系统设置”链接，弹出“高级系统设置”对话框。

STEP 03　打开“高级”选项卡，然后在“用户配置文件”选项下单击“设置”按钮。

STEP 04　随后可看到如图 1-30 所示的“用户配置文件”对话框。

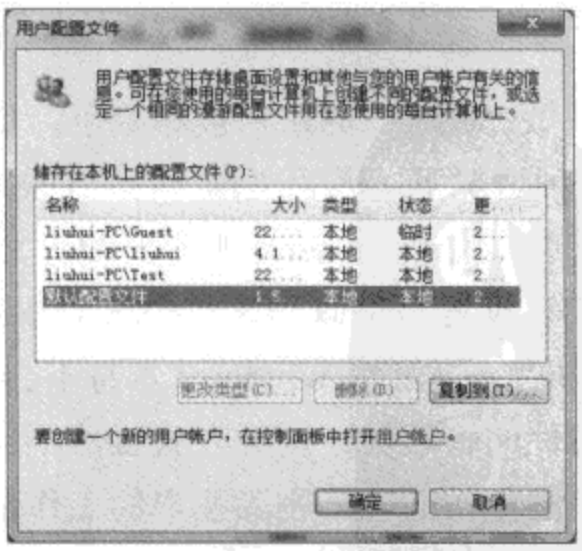


图 1-30　在这里可看到每个本地账户的配置文件信息

STEP 05 选中“默认配置文件”，并单击“复制到”按钮。

STEP 06 在随后出现的“复制到”对话框中单击“浏览”按钮，选定目标账户的配置文件所在的位置。选择好之后单击“确定”按钮，回到“复制到”对话框，再次单击“确定”按钮。

经过这样的操作，当我们再次使用该账户登录后，就可以看到类似新账户一样完全是默认配置的桌面环境。但是需要注意，这样做有可能导致重要的数据被删除，例如用户保存在自己的“文档”文件夹下的重要文件，或者 Internet Explorer 收藏夹。简而言之，所有保存在用户配置文件中的数据都会被删除。因此，如果有重要文件需要保留，必须在删除账户之前将其移动到其他地方。

对于配置文件，还有一个有关账户删除的问题需要注意。如果我们需要删除某个不再需要的账户，那么在处理该账户的配置文件时就需要谨慎，因为不同的操作可能导致不同的后果。

如果从控制面板的用户账户工具下删除，那么在删除的时候，Windows 会弹出如图 1-31 所示的对话框询问我们是否删除该账户的文件。如果决定删除文件，那么可以单击“删除文件”按钮，否则可以单击“保留文件”按钮，这样 Windows 会自动将该用户的私人文件复制到当前用户的桌面上。但如果是从计算机管理控制台的本地用户和组管理单元中删除账户，情况就不太相同了。为了保证数据的安全性，在本地用户和组管理单元中删除时，Windows 不会询问，而是直接保留被删除账户所有的配置文件。这听起来很正常，但有时候有可能带来新的问题。

图 1-31　询问是否保留该账户的私人文件

假设系统中曾经有一个叫做“User”的账户被删除了，后来因为某些原因，又要新建一个名为“User”的账户。这种情况下，因为之前一个“User”账户的配置文件还保留着，因此，新建的“User”账户无法使用老“User”账户的配置文件，此时，Windows 会将新“User”账户的配置文件夹的名称设置为类似“User.XXXXXX”的形式，其中，“XXXXXX”是机器名的一部分，是一串随机字符。虽然 Windows 本身不会被名称相似的配置文件弄混，但是对于需要手工管理配置文件的管理员，这种方式显然不够好，不仅不直观，而且手工操作配置文件的时候会感到很混乱。因此，删除账户的工作最好在控制面板的用户账户工具中进行，这样可以根据需要选择是否删除账户的配置文件，同时，如果一定要用本地用

户和组管理单元管理账户和配置文件，最好在管理后手工处理保留的配置文件。

1.3.4　其他选项

对于 Windows 操作系统安装好后初步的安全问题，基本就是这样了。在本书后面的章节中，我们还会重点介绍其中比较关键的一些问题，但在这之前，还有几个问题需要注意。

1.3.4.1　自动播放

曾经有一种病毒大出风头，作者在写这本书的时候，时间已经过去很久了，但我们依然能在不少地方见到这种病毒的身影，这就是俗称的“U 盘病毒”，这个病毒是利用 Windows 的自动播放功能传染和传播的。

自动播放本来是一个很好的功能，可以检测可移动存储介质的存在，以及其中保存的文件内容，并自动提供方便我们使用的选项。例如，启用自动播放功能后，如果将 DVD 影碟放入光驱，Windows 检测到了 DVD 影碟的存在，就会打开“自动播放”对话框，其中的选项则取决于系统中安装的软件，例如可以使用 Windows 自带的 Windows Media Player，或者自己安装的其他兼容的播放器播放 DVD 影碟的内容，或者打开 Windows 资源管理器窗口查看光盘内容；如果将数码相机的存储卡插入读卡器，Windows 的“自动播放”对话框就会提供导入图片、查看图片等选项；如果将软件的安装光盘放入光驱，Windows 的“自动播放”对话框则可以提供查看光盘文件或者运行安装程序的选项。

可以说，自动播放功能简化了我们很多的日常工作，但这也容易带来隐患，例如 U 盘病毒。如果我们的可移动存储介质感染了病毒，那么当这种存储介质连接到计算机后，自动播放功能就会自动运行病毒，感染计算机，并感染其他没有染毒的可移动存储介质。

被 U 盘病毒感染的可移动存储介质的根目录下会保存一个名为“autorun.inf”的文件，该文件中则指向了一个可执行的.exe 文件。而根据设计，以前 Windows 一旦检测到可移动存储介质的根目录下存在 autorun.inf 文件，就会自动执行该文件指定的可执行文件。因此，一旦原本无毒的计算机中连接了感染病毒的存储设备，很可能我们还来不及反应，自己的系统就已经被感染了。

如果系统已经中了这种病毒，请使用升级了最新病毒定义的反病毒软件查杀，详细信息请参考本书第 10 章的相关内容。下面我们将介绍怎样预防这类病毒感染计算机。

对于 Windows 7，情况就简单多了，因为 Windows 7 在这方面有很多改进。首先，就算一个可移动存储设备中包含 autorun.inf 文件，Windows 7 也会首先询问我们需要对设备采取怎样的操作（例如运行其中的软件，或浏览设备的内容），而不会自作主张地直接运行。另外，通过“控制面板”中提供的选项，我们完全可以控制自动播放的所有设置。

打开“控制面板”，依次进入“程序”→“默认程序”→“更改自动播放设置”，随后可以看到如图 1-32 所示的自动播放设置界面。

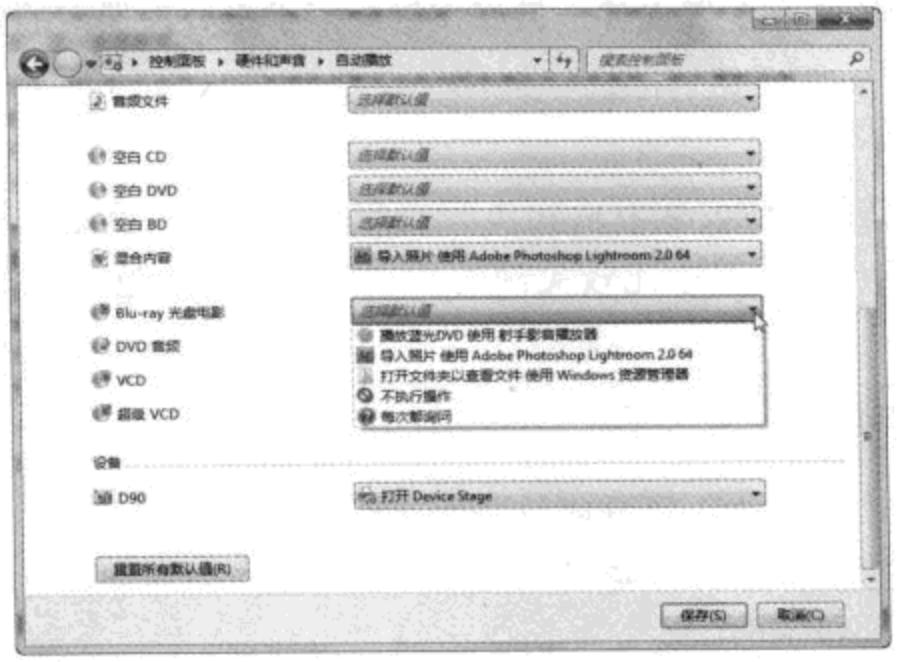


图 1-32　利用控制面板中的选项设置各种介质的自动播放选项

如果希望彻底禁用自动播放功能，只需要反选窗口顶部的“为所有媒体和设备使用自动播放”选项即可。

另外，Windows 会列出可以支持自动播放功能的所有媒体和设备类型，每个类型或者设备都有一个对应的下拉菜单，打开该菜单可以看到当前系统对这种媒体类型或者设备可以进行的操作。具体的操作内容取决于系统中安装的软件，因此，每个人看到的内容可能和图 1-32 所示的不完全相同。

除了可以针对不同种类的可移动存储设备进行设置外，在 Windows 7 中还可以针对具体的硬件设备进行设置，例如，我们可以设置将某一型号的相机连接到计算机后，采取怎样的自动播放选项；而如果只是将相机使用的存储卡连接到计算机，又采取怎样的选项。

对于每种类型或设备，只需要在对应的下拉菜单中选择希望使用的选项即可。这里需要注意的是“软件和游戏”这种类型，因为 Windows 7 还没有智能到知道我们提供的光盘或 U 盘中的内容是否是软件或游戏的安装文件。因此，如果检测到介质中包含 autorun.inf 文件，或者其他可执行文件，那么就会将该介质识别为“软件和游戏”，而实际上这可能只是一个染毒的 U 盘。在此建议将“软件和游戏”类别设置为“每次都询问”或“不执行操作”，这样相对更加安全一些，同时其他类型介质的自动播放不会受到影响。

“混合内容/增强型音频 CD/增强型 DVD 电影”又是什么意思？现在有一种新型的光盘，原本只是音频 CD 或视频 DVD，但发行商为了增加卖点，会在光盘中添加一些小功能，例如音频 CD，它不仅可以在一般的 CD 唱机中播放，而且在计算机上使用的时候还可以玩其中的游戏，或者观看 MV。这种包含多种不同类型功能的介质叫做“混合内容/增强型内容”。这个功能原本只是为了增加产品的附加值，但有时候容易被造成滥用，例如，2005 年底名噪一时的新闻，SONY 唱片公司给自己发行的很多音乐 CD 中预置了一种叫做 Rootkit 的软件，这类软件会在我们将 CD 唱片放入计算机光驱后自动运行，安装并潜伏到系统中，主要是为了防止非法复制唱片。但这种 Rootkit 软件比较隐蔽，无法卸载，因此，SONY 的这

种做法引起了轩然大波，其实这种包含 Rootkit 的 CD 唱片就是一种“增强型音频 CD”，那么对于这类介质该怎样设置自动播放选项，相信大家都已经很清楚了。

设置好所有类型和设备的自动播放选项后，单击“保存”按钮可以保存更改，或者单击“重置所有默认值”按钮可以将所有的选项恢复为默认设置。

1.3.4.2　Syskey

上文已经介绍了怎样使用软件对 Windows 系统进行脱机攻击，破解本地账户的密码。那么怎样预防这类攻击？对于 Windows 7 企业版和旗舰版，可以使用 BitLocker（关于该功能的详细信息，请参考本书第 12 章），如果用的 Windows 7 是其他版本，且不支持该功能，有什么好办法吗？

还是让我们再来回忆一下 Windows 操作系统保存用户登录信息的方式，以及脱机破解密码软件的工作原理吧。在单机或工作组环境下，每个本地账户的登录信息（用户名和密码）都是加密保存在 SAM 文件中的，而 Winlogon 进程会将我们在欢迎屏幕或者 Windows 登录对话框中输入的用户名和密码与 SAM 数据库中存储的信息进行对比，如果能找到匹配的项目，就认为用户提供的登录信息是有效的，允许登录；如果找不到匹配的信息，则会拒绝登录。

脱机破解密码的软件正是利用了这一点，在 Windows 没有运行的情况下访问 SAM 数据库文件，并根据一些复杂的算法强行进行破解或修改。那么可以考虑，如果将 SAM 文件进行再次加密，并将解密所需的信息保存在计算机以外的地方，是否就可以防范这种脱机破解呢？答案是肯定的。

这里要用到 Syskey.exe，这是 Windows 系统自带的一个工具。启用该功能后，SAM 数据库会被再次加密，同时加密后的信息会被保存到软盘上。这样，在需要使用计算机的时候就必须提供这张保存了机密信息的软盘，随后，Windows 才可以利用软盘中的信息解密 SAM 数据库，并接受登录。如果无法提供软盘，SAM 数据库依然处于加密状态，自然也就无法登录了。

Syskey.exe 可用于 Windows 2000/XP/2003/Vista/7 系统，并且在这些系统中的操作方式都是一样的。

在继续操作之前，请确定计算机上装有软驱，并且手头有空白的被格式化过的软盘。很令人费解，现在配备软驱的计算机已经很少了，毕竟软盘的容量小、速度慢，可靠性还差，但这里只能使用软盘。为了避免软盘损坏后无法使用系统，在创建好这张“密钥盘”后，建议直接将其中的文件复制到别的软盘中以进行备份，这样一张软盘损坏了，还可以使用其他软盘应急。同时请注意，一定要将密钥盘和密钥盘的备份保存在安全的地方。另外，该功能一旦启用，就无法禁用，除非重装操作系统或者进行系统还原。

如果不使用外部设备，还可以通过设置额外一层密码的方式使用该功能。我们可以指定一个密码，将 SAM 数据库加密。这样等于在系统启动时首先需要输入一个解锁 SAM 数

据库的密码，随后选择用户账户，并输入账户密码，以便正确登录。因此，为了方便起见，这里会介绍使用密码进行加密的方式。对于使用软盘保存密钥的方式，可操作性太低，这里不再介绍。

STEP 01 打开“开始”菜单，在搜索框中输入“Syskey”后按回车键，即可打开该程序。

STEP 02 在随后出现的“保证 Windows 账户数据库的安全”对话框中，确保已经选中了“启用加密”选项，然后单击“更新”按钮，随后可以看到如图 1-33 所示的界面。

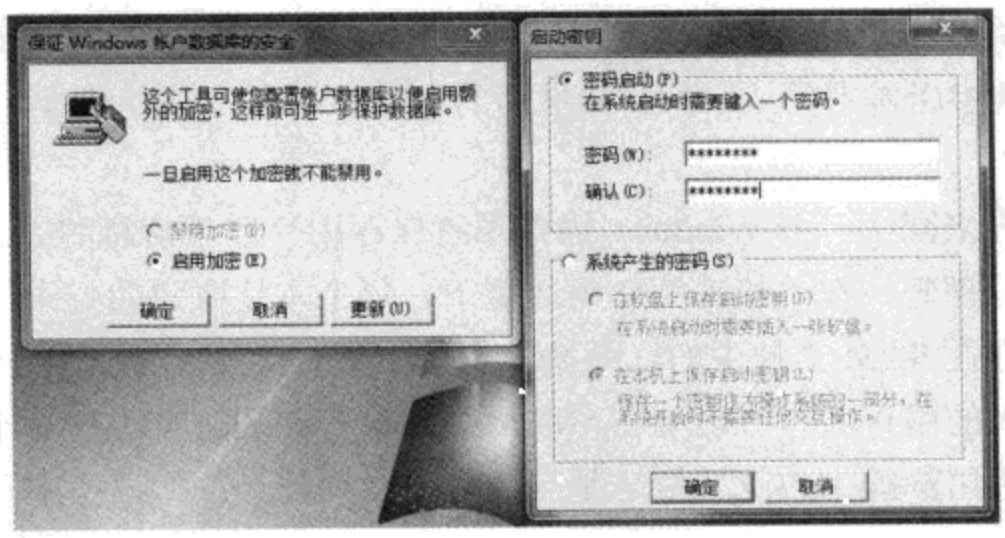


图 1-33　使用 Syskey 功能对 SAM 数据库进行加密

STEP 03 因为需要在没有软驱的情况下使用，因此，这里可以选择“密码启动”，并输入一个密码（这个密码一定要牢记，并且一旦对 SAM 进行加密，就无法撤销，但如果有必要，可以再次运行 Syskey，修改密码）。这里使用的密码不能与 Windows 账户的密码相同，否则安全性会降低。

STEP 04 随后单击“确定”按钮两次，关闭该工具。

让我们看看对 SAM 进行加密可以怎样保护我们的账户安全。重新启动系统，当系统开始引导、加载后台服务之前，首先就会要求我们输入启动密码，否则根本无法看到登录界面（如图 1-34 所示）。该功能一经启用，就算要进入安全模式，也必须首先输入密码才能继续。

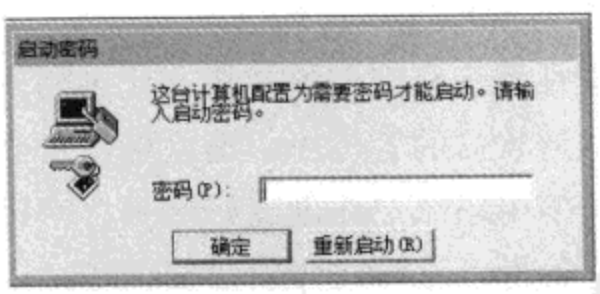


图 1-34　必须输入正确的密码后才能看到登录界

因为启用 Syskey 后无法禁用，因此，如果日后不再需要如此高的安全性，这时可以考虑将启动密钥保存在硬盘上，这样，Syskey 依然处于启用状态，但是至少不要求我们在系统启动的时候提供密钥了（无论是手工输入密码，还是提供保存了密钥的 3.5 寸软盘）。切换 Syskey 工作方式的方法很简单，正常启动系统，并使用管理员账户登录，运行 Syskey，在图 1-31 所示的界面上选中“启用加密”，单击“更新”按钮，然后选中“系统产生的密码”，并选择“在本机上保存启动密钥”选项，并输入目前使用的启动密码即可。

经过上述操作，SAM 数据库实际上依然被加密保存，只不过解密所需的密钥已经保存到本地硬盘上，因此，启动系统的时候可以直接看到登录界面。

1.3.4.3　操作中心

对于一般用户，可能很难判断出自己的系统当前是否是安全的，因为有太多因素会影响系统的安全性，例如，是否安装了反病毒软件，反病毒软件的实时监控功能是否被启用，病毒定义是否被更新到最新，是否安装了网络防火墙，网络防火墙是否被启用，系统的安全设置是否存在问题等。

若是以前，我们必须打开多个程序，并查看大量选项的设置，才能了解系统的整体安全性，这样不仅麻烦，而且容易造成遗漏。自从 Windows XP SP2 开始，微软在 Windows 中增加了一个叫做“Windows 安全中心”的功能，这是一个后台运行的服务，会密切监控系统中与安全有关的程序和设置，一旦发现有威胁到安全的事件，就会立刻发出警报提醒我们注意，并提供相应的解决方法。

Windows 7 中的安全中心已经全面升级为“操作中心”，它不仅可以显示与系统安全性有关的提示信息，而且还增加了有关系统维护的内容，更加全面。下面将介绍操作中心中与安全有关的内容。

> **注意**　Windows 操作中心功能并不是安全软件
>
> 很多人认为，如果有 Windows 操作中心的存在，是否就意味着安全问题可以交给它，而我们不用安装和设置其他安全软件。这是完全错误的。Windows 操作中心只是一个监控程序，它可以监控系统的安全状态，并在需要的时候发出警报提醒我们注意，而它并没有任何安全防范功能。例如，如果系统中存在病毒，还是需要依靠反病毒软件查杀，操作中心只能告诉我们系统中是否安装了反病毒软件，以及病毒定义是否过期。

全新安装好 Windows 后，可能很快就会看到操作中心警报（如图 1-35 所示），因为它会提醒我们系统中没有安装反病毒软件，或者病毒定义过期。按照提示安装好反病毒软件或更新病毒定义后，操作中心程序就开始在后台工作。很多人可能觉得，如果系统已经完全满足操作中心的要求，需要的软件都安装了，需要的设置也都设置好了，那以后是否可以禁用该功能，以节约系统资源。在这里建议尽量不要这样做，因为有时候可能会有恶意软件修改我们的系统设置，让原本安全的系统变得不够安全。这时候，正常情况下的反病毒软件是需要干预的，然而一旦发生漏报，就会直接危害到系统安全。如果启用了操作中心，系统会立刻提醒我们系统的安全设置发生了改变；如果将其禁用，我们可能就会在很长一段时间内在毫无察觉的情况下进行在线交易或者网上支付等活动，危险不言而喻。

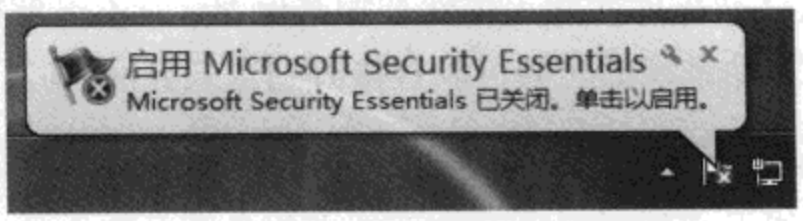


图 1-35　操作中心会告诉我们系统中存在的安全隐患

单击桌面右下角通知区域内的操作中心图标后，可以看到类似图 1-36 所示的弹出菜单，这里会列出所有可能存在的问题。单击对应的条目，即可查看详细信息，以及建议的解决方法，例如，如果没有安装反病毒软件，那么操作中心会提供获取这些软件的方法；如果反病毒软件被禁用，直接单击操作中心提供的按钮就可以将反病毒软件启用，或者对其进行更新。

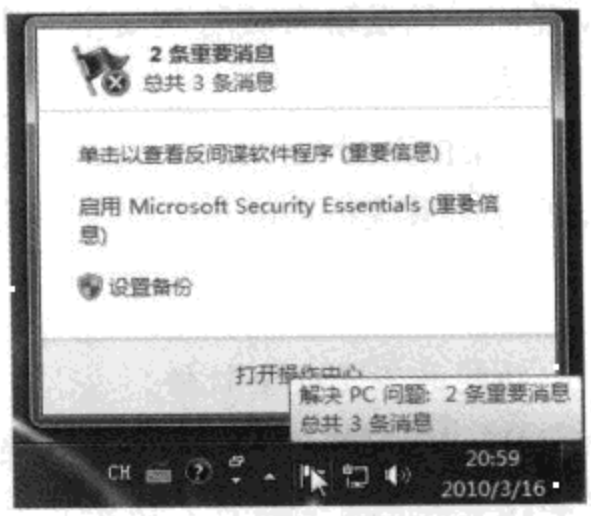


图 1-36　从弹出菜单中可直接查看多个需要注意的问题

在图 1-36 所示的界面中单击“打开操作中心”链接后，即可看到操作中心主界面（如图 1-37 所示）。上文已经提过，操作中心可以提示有关安全性，以及维护工作的相关事件，从图 1-37 中也可以看出，这些内容被划分为“安全”和“维护”两个类别。默认情况下，这两个类都是被合并的，只有需要注意的问题才会突出显示出来，并且取决于问题的严重程度，不同的问题会用不同的颜色进行标识。红色通常意味着可能严重影响系统安全性或稳定性的问题，需要尽快着手解决；黄色意味着问题虽然存在，但影响不会太大，不过依然有必要解决，取决于具体的问题，我们需要单击对应的操作按钮进行解决。例如，图 1-39 所示的病毒防护软件被关闭，那么这里就提供了“立即启用”按钮，单击它即可将该软件启动。

单击打开“安全”类别后可以看到，Windows 7 的操作中心可以监控多个与安全有关的内容，这些内容包括：

- **网络防火墙**　默认情况下，该项目会检测 Windows 防火墙的状态，查看该防火墙是否启用，如果被禁用，则提供启用 Windows 防火墙的选项。如果系统中安装了第三方网络防火墙软件，并且支持安全中心所用的 WIM 标准，那么从这里就可以监控安装的其他防火墙。有关 Windows 防火墙的详细信息，请参考本书第 8 章。

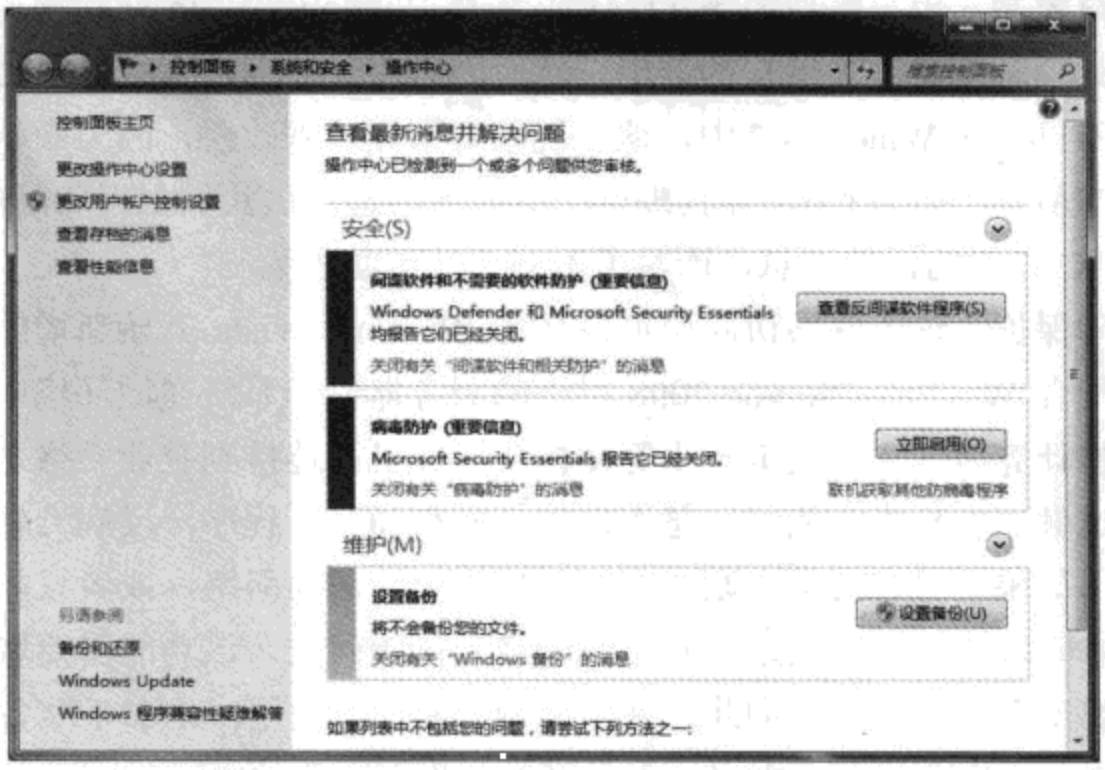


图 1-37　Windows 7 操作中心的主界面

- **Windows Update**　这里可以检测 Windows Update 是否启用，以及是否使用了推荐的设置。如果没有启用，或者没有使用推荐设置，这里就会用不同的颜色进行区别。有关自动更新和 Windows Update 的详细信息，请参考本书第 4 章。
- **病毒防护**　这里可以检测系统中是否安装了反病毒软件，以及软件的状态。如果没有安装，则通过这里提供的按钮，我们可以在网页中查看微软推荐的所有反病毒软件。如果已经安装，但没有启用，或病毒库定义过期，则可以通过这里提供的选项直接启用反病毒软件，或更新病毒库定义。
- **间谍软件和不需要的软件防护**　除了病毒，网上还有一些不受欢迎的程序，由于这些内容的破坏性不强，因此，很多人将其称之为间谍软件或恶意软件。Windows 7 中自带了微软的反间谍软件 Windows Defender，该项目对应了这个软件的相关信息。另外，很多第三方的反病毒软件往往具有反间谍软件功能，或者我们可能安装其他第三方的专门反间谍软件，这种情况下，取决于软件对操作中心功能的支持情况，也可以从操作中心直接查看软件的状态，或对其进行管理。有关反病毒软件以及防范恶意软件的详细信息，请参考本书第 10 章。
- **Internet 安全设置**　Windows 7 包含 Internet Explorer 8 浏览器，这是迄今为止微软提供的最安全的浏览器软件，该软件的大部分设置都是以保持安全性为首要目标的。但由于各种原因，Internet Explorer 选项的安全性可能会降低，例如，为了浏览某些网站，我们可能需要将原本安全的设置修改为不太安全的状态；或者系统中感染了恶意软件，可能会偷偷修改 Internet Explorer 配置。此时可使用操作中心对 IE 的安全状态进行监控，一旦发现配置被改动，即可立刻发出警报，并提供用于纠正问题的选项。有关 Internet Explorer 安全性的相关内容，请参考本书第 9 章。

- **用户账户控制** 用户账户控制（UAC）是从 Windows Vista 开始增加的一个功能，可以有效地防范管理员特权的滥用。然而因为各种原因，大家对该功能的评价并不太好。不过，在 Windows 7 中，这一现象将彻底得到改善，因为微软已经重新设计了整个 UAC 功能的行为，并且提供了更细致的选项供我们根据实际情况进行调整。有关 UAC 功能的详细信息，请参考本书 2.2 节的内容。
- **网络访问保护** 这个网络访问保护也是从 Windows Vista 开始新增的功能，但该功能需要配合 Windows Server 2008 以上的服务器操作系统在域环境中使用。简单来说，在将计算机（主要是笔记本等便携式计算机）连接到企业网络之前，系统首先需要通过健康度检查，例如，是否安装了所有的补丁程序，反病毒软件定义是否为最新等。如果不符合要求，则这台计算机将无法访问网络，或者只能访问网络中被隔离的修补服务器，并通过修补服务器修复健康问题。该功能需要域环境的支持，并且需要专门的服务器，因此，并不适合一般用户使用，本书不准备过多涉及。

操作中心中有关安全问题的内容，主要可以分为下列几种情况：

对于缺少的软件，例如缺少网络防火墙、反病毒软件或者反间谍软件，只要安装了支持 WIM 的软件，然后重新启动系统，操作中心就可以识别出新安装的软件，并更新相应类别的状态。但如果自己不知道有哪些安全软件是兼容 Windows 7 的，例如，还没有安装反病毒软件，希望使用一个微软推荐的软件，则可以单击相应的类别（例如，反病毒软件对应的“恶意软件保护”类别），然后单击“查找程序”按钮，这样系统会自动调用浏览器访问微软网站上的相关页面，在那里可以看到微软推荐的所有软件，并可下载和试用。

对于错误的设置，操作中心则会在对应的类别下提供一个“还原设置”按钮，只要单击这个按钮，不用知道具体有哪些设置需要改变，操作中心就会自动将不安全的设置修改为推荐的安全的设置。

如果已经安装了反病毒软件，但操作中心无法检测到该软件的存在，依然报告说没有安装反病毒软件，这时候可以单击对应类别下的“关闭有关×××的消息”链接，这样的内容就会被操作中心隐藏，不再反复提示。

另外还可能存在一种情况，为了满足使用上的特殊需要，我们可能需要使用一些不够安全的设置，例如，确实需要禁用用户账户控制功能（虽然强烈推荐不这样做），或者确实需要使用不够安全的 Internet Explorer 设置，但操作中心总会频繁地告诉我们这样做不够安全，显得有些烦人。这时候我们可以告诉操作中心，自己需要它监视哪些类别的安全问题，同时忽略哪些类别的安全问题。方法很简单，只要单击操作中心主窗口左侧的“更改操作中心设置”链接，随后可以看到如图 1-38 所示的界面。

在这里可以根据实际需要进行选择，例如，如果不希望操作中心频繁通知我们已经知道的安全问题，可将对应的类别反选。如果随后希望重新看到相关类别的通知，也只需要在这里将其选中即可。

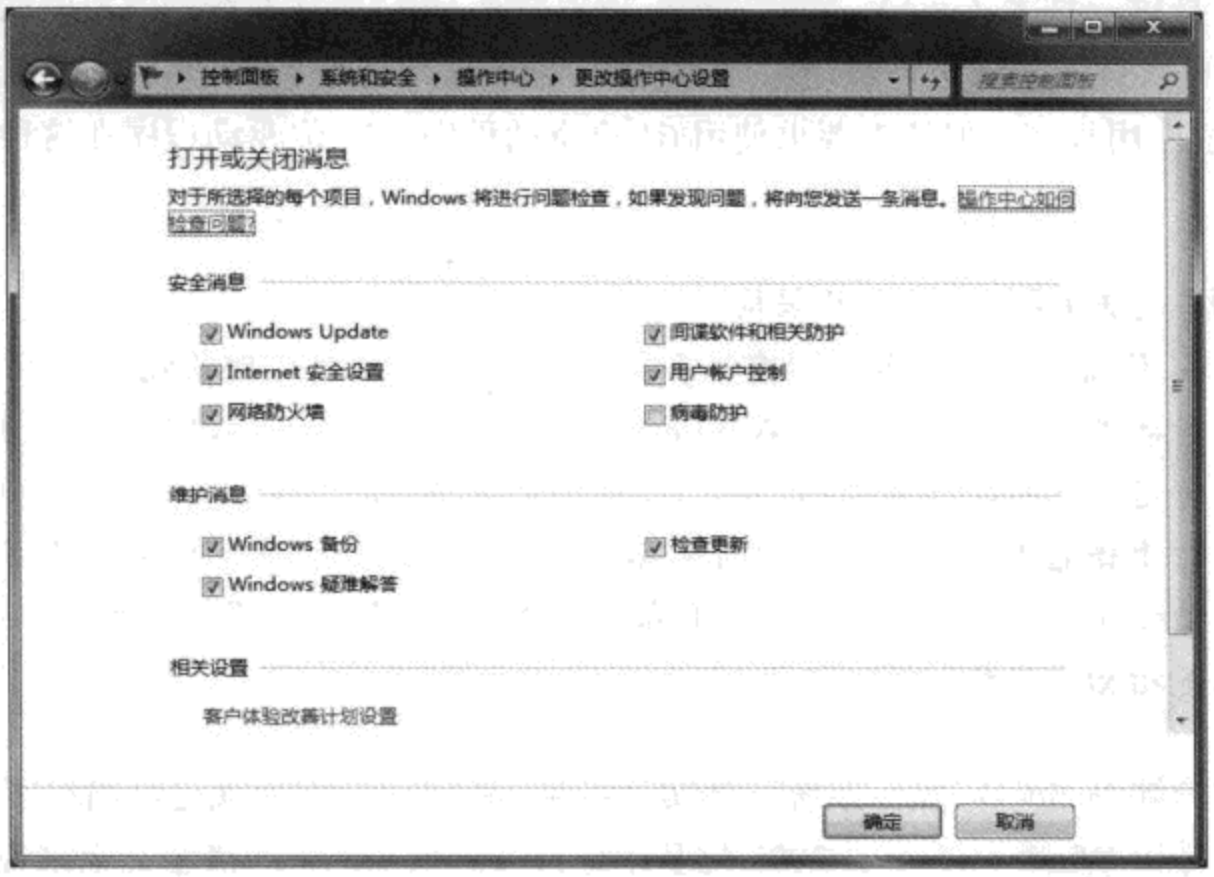


图 1-38　更改操作中心的工作方式

1.4　其他安全功能

除了下文通过不同章节介绍的安全功能之外，在 Windows 7 中，还有一些安全方面的改进值得注意。但由于这些改进的大部分都是在内核层面上实现的，我们并不容易直观地察觉，当然也没有过多的选项可供配置相关的功能。因此，在本章末尾，我们将简要介绍有关内核和 Windows 内部的安全改进，这些改进在 Windows 底层默默无闻地改善着我们的系统安全。

1.4.1　更安全的 64 位系统

当前，64 位计算是一个很流行的话题，那么到底什么是 64 位计算？相比传统的 32 位计算，有什么好处？又有什么不足？

这里所说的“64”位和我们常见的“32”位，都是指计算机系统总线的长度，简单来说，也就是一次可以处理的数据量。很明显，64 位系统可以处理比 32 位系统多一倍的数据。在具体的表现上，最明显的变化就是可以支持更多的物理内存。在客户端 Windows 领域，32 位版本的 Windows 最多只能对 3GB 多的物理内存寻址，也就是说，如果计算机的物理内存超过 3GB，超出的部分将无法被操作系统和应用程序使用。虽然在 Windows Vista SP1 以及 Windows 7 中，32 位系统可以在系统属性等界面显示出超过 3GB 的内存，但并不意味着这些额外的内存可以被使用。

要获得 64 位环境，必须有 64 位的处理器，现阶段，AMD 以及 Intel 的主流处理器基

本都已经支持这一技术（x64）。除此之外，还需要有 64 位操作系统，以及驱动程序和软件的配合。对于 x64 架构（也是普通用户所能接触到的唯一 64 位架构环境）系统，可以运行大部分 32 位应用程序，但依然要求使用 64 位驱动程序，32 位驱动程序在这种情况下根本无法安装。

> **注意** 有关 64 位处理器的架构
>
> 64 位架构的处理器类型有很多，例如，Intel 的安腾处理器就使用了 IA-64 架构，但这种硬件需要专用版本的 Windows 系统，主要用于服务器以及高端工作站等领域，不是普通用户所能接触到的。
>
> 对于普通用户，最常见的则是 x64 架构的处理器，这种环境下使用的操作系统和驱动程序，以及应用程序通常更容易获得。若无特别注明，本书所提到的 64 位环境都是指 x64 架构环境。

对于客户端 Windows 操作系统，其实早在 Windows XP 时代就已经出现了 64 位版本，不过该系统是以 Windows Server 2003 位基础进行改进而来的，严格意义上来说，并不是原生的客户端 64 位 Windows 系统。从 Windows Vista 开始，微软分别提供了 32 位和 64 位客户端 Windows 系统，Windows 7 也是如此。

现阶段，64 位系统最大的不足在于驱动程序和应用程序的兼容性。虽然经过 Windows Vista 的铺垫，软硬件厂商都开始重视 64 位环境的要求，并开始提供 64 位的驱动程序，但兼容性问题依然存在。应用程序的兼容性问题还很简单，因为大部分 32 位应用程序都可以在 64 位系统中正常运行，但缺乏相应的驱动程序，硬件无法正常工作，这一点自然是无法接受的。因此，在 Windows Vista 时代，64 位环境主要出现在对性能有较高要求的专业用户中，普通用户很少会用这种系统。

从 Windows 7 开始，情况有了很大好转。对于大部分主流的硬件产品，基本上都有了 64 位驱动，而且 64 位应用程序也越来越多。再加上硬件技术的发展，尤其是大内存（超过 3GB 内存）用户的增加，64 位也开始逐渐走进普通用户的桌面。

在 Windows 7 中，要判断自己的系统环境是 32 位或者 64 位，可以打开“开始”菜单，用鼠标右键单击“计算机”，选择“属性”，打开如图 1-39 所示的系统属性窗口，在“系统类型”一栏中，即可知道自己的操作系统类型。

在使用 64 位环境后，除了可以使用更多的内存外，还有很多其他的好处，最主要的可能就是一些需要较大运算量或内存占用多的专业程序，例如图形和视频处理、编辑软件、数据库应用等。因为应用程序在 64 位环境下可以使用更多的内存，并且处理器的总线更宽，数据的传输速度更快。因此，在一些专业领域，如果能配合使用 64 位应用程序，操作效率将得到大幅度提高。

那么对于普通用户，如果不需要处理大量的数据，不需要使用大量的内存，64 位是否

毫无价值？其实也并不是这样，它可以获得更好的安全性。对于 64 位 Windows，因为使用了与传统的 32 位系统完全不同，并且更先进的内核，因此，可以从中获得大量有关安全性的改进，就算是普通用户，如果可以使用 64 位环境，系统的安全性也将得到很大的提高。本节将简要介绍这些改进，注意，这些改进是 64 位 Windows 7 独有的。

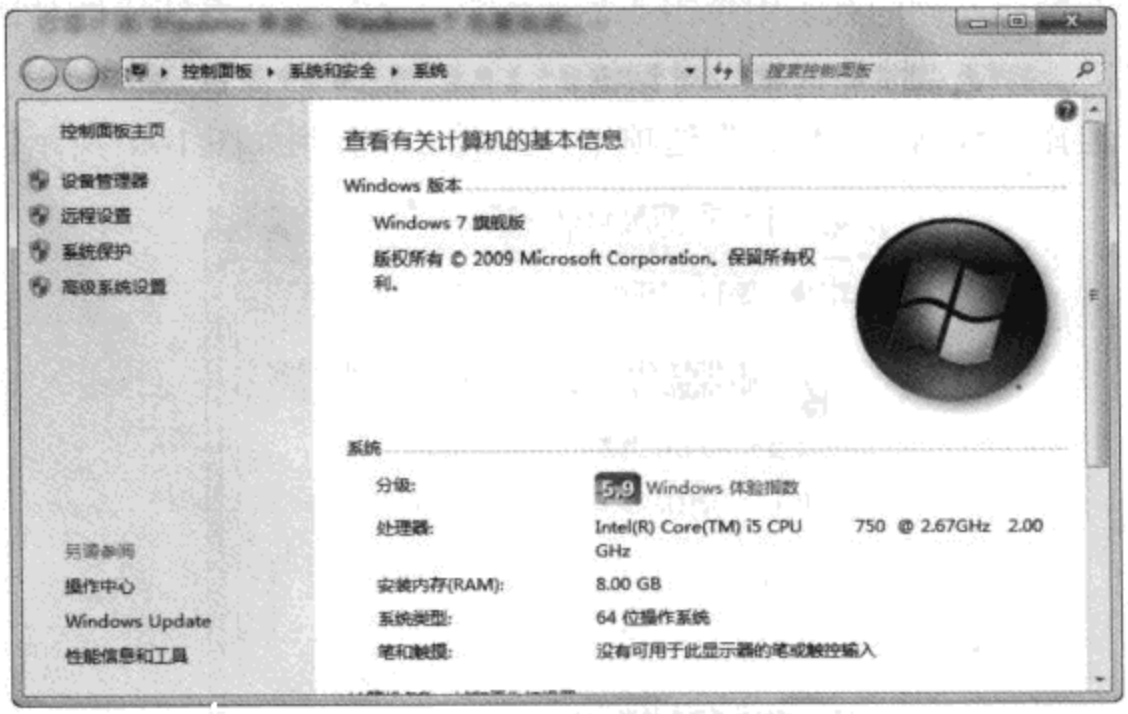


图 1-39　通过系统属性窗口可知道自己的系统类型

1. 数据执行保护

在对计算机系统进行攻击时，缓冲区溢出攻击是一种很常见的做法。缓冲区是在内存中划分出的一块供应用程序临时存储数据的区域，每个应用程序可以使用的缓冲区大小是固定的，而一旦应用程序尝试给缓冲区中写入超过固定大小的数据，就会导致缓冲区溢出，这将导致超出缓冲区大小的数据会覆盖掉内存中的其他非缓冲区数据。这个就像是一个水池，装水的容量是固定的，如果一定要装入更多的水，那么自然会溢出到水池外。

因此，攻击者可能会尝试输入超出应用程序可接受范围的数据的方式，在系统内存中产生缓冲区溢出现象，而如果攻击者的技术水平够高，就会使得“溢出”的数据成为某种指令，让操作系统执行某些恶意代码，并且这一执行工作是按照被溢出的程序的特权级别来运行的。可想而知，如果是 Windows 系统本身，或者某些需要高特权的应用程序存在缓冲区溢出漏洞，攻击者将使用非常高的特权执行自己的恶意代码，并导致严重的后果。

为了防范这种攻击方式，从 Windows XP SP2 开始，微软提供了数据执行保护（Data Execution Prevention，DEP）功能，该功能会将内存区域按照所保存内容的不同，明确标注为“数据代码”或“应用程序代码”，对于“数据代码”区域中的内容，操作系统是绝对不会执行的，而通常用户所输入的或者通过网络获得的数据，都会保存在“数据代码”区域中。因此，通过这种方式可以彻底防范缓冲区溢出攻击。

其实，32 位 Windows 中也包含 DEP 功能，不过是通过软件形式实现的，而 64 位 Windows 则可以充分利用 64 位处理器所包含的硬件 DEP 功能，在硬件层面上实施 DEP 保护。因此，

这样的保护更难以被攻破。

要配置 Windows 7 的 DEP 功能，请按照下列步骤操作：

STEP 01 打开“开始”菜单，在“计算机”上单击鼠标右键，选择“属性”，打开系统属性窗口。

STEP 02 在窗口左侧的列表中单击“高级系统设置”，打开系统属性对话框，单击第一个“设置”按钮，打开“性能选项”对话框。

STEP 03 选择“数据执行保护”选项卡，随后可以看到如图 1-40 所示的内容。

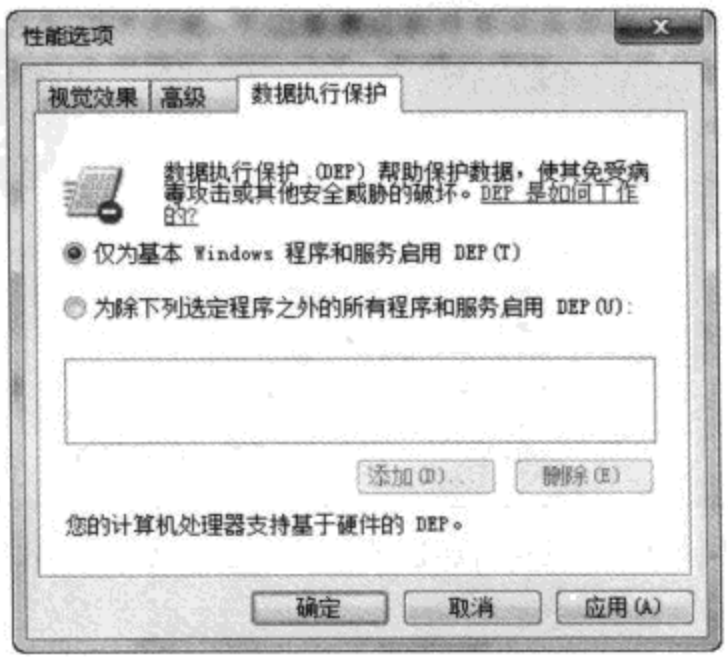


图 1-40　配置操作系统的 DEP 功能

STEP 04 在对话框底部可以看到本机所能支持的 DEP 模式。如果使用了 64 位处理器，那么从这里可以看到，本机支持“基于硬件的 DEP”，否则将显示为“基于软件的 DEP”。

STEP 05 默认情况下，系统只针对重要的 Windows 服务和内建程序启用 DEP 功能，我们安装的其他应用程序将无法受到保护。因此，如果希望获得更全面的保护，可以选中“为除下列选定程序之外的所有程序和服务启用 DEP”选项。

STEP 06 通过上述设置，系统中运行的所有内容都将受到 DEP 的保护。然而该功能存在一定的问题，如果某个程序的编写不够完善，即存在 Bug，可能导致完全无法正常运行，或者运行一段时间后自动出错并退出的情况。因此，在进行上述设置后，如果发现某个程序开始出错，可以将其添加到列表中，这样系统就不会对该程序启用 DEP。为此，只需要单击“添加”按钮，并将该程序的可执行文件（.exe）添加到列表中即可。

DEP 功能可以有效地防范缓冲区溢出攻击，然而需要提醒注意的是，缓冲区溢出攻击并非唯一的攻击方式，因此，不能因为启用了 DEP 就不使用其他安全软件。反病毒软件、反间谍软件，以及网络防火墙等安全工具的使用还是很有必要的。有关这些内容的介绍，请参考本书第 10 章。

2. Kernel Patch Protection

所有 64 位版本的 Windows 都支持 Kernel Patch Protection（KPP，内核补丁保护）技术。KPP 技术可以防范未经授权的软件对 Windows 内核执行的修补操作，因此，可以进一步增强涉及整个系统的性能、安全性，以及可靠性的 Windows 内核的安全。KPP 功能可以检测对内核内存中重要位置的改动操作，如果改动是通过未经授权的方式（例如用户模式的应用程序试图恶意调用某些操作系统函数）进行的，那么，KPP 会立刻生成一个 STOP 错误（也就是让整个操作系统蓝屏挂起），防止系统内核被恶意修改。同时，该功能还可防范内核模式的驱动（要知道，很多病毒或恶意软件为了感染或驻留在系统中，往往会给系统中安装驱动程序）影响到重要的内核服务，或者其他第三方软件更改系统内核。

根据微软的介绍，如果驱动程序尝试执行下列操作，KPP 功能将会生成 STOP 错误：

- 修改系统服务表。
- 修改中断描述表（Interrupt Descriptor Table，IDT）。
- 修改全局描述表（Global Descriptor Table，GDT）。
- 使用并非由内核所分配的内核堆栈。
- 在 AMD 64 架构的系统中对内核进行任何形式的更新。

由此可见，在正常运行 Windows 的过程中所遇到的蓝屏死机，并非总是代表系统不稳定，有些情况下属于系统的自我保护手段。因此，如果遇到蓝屏死机问题，还需要结合错误信息仔细分析。

对于普通用户，KPP 没有任何可供配置的选项。不过一定要确保自己使用的所有设备驱动都是符合要求的。

3. 驱动强制签名

对于 NT 架构的操作系统（例如 Windows 2000/XP/2003/Vista/2008/7）本身已经非常稳定，但很多人在使用过程中依然会遇到各种各样奇怪的问题，甚至蓝屏死机。实际上，这些问题大部分情况都是由于硬件故障、第三方软件编写不完善，或者有 Bug 的驱动程序导致的，而驱动程序的问题可能是其中最重要的。

驱动是一种特殊的程序，往往要工作在操作系统的内核中才能让操作系统以及其他软件正确使用硬件设备。而这也就导致驱动几乎可以不受限制地访问任何系统资源。因此，如果使用的驱动编写有问题，或存在 Bug，或者系统中被安装了包含驱动的恶意软件，可能会对系统的稳定性和安全性产生很大影响，而这一点在任何操作系统上都是一个不可避免的问题。

对于普通用户，在 Windows Vista 刚发布的时候可能已经深刻了解到驱动可以对操作系统产生的影响。在 Windows Vista 刚发布的时候，如果运行国内某个非常著名的聊天软件，只要在该软件的登录界面上单击密码输入框，输入密码，系统会立刻蓝屏死机，其实这就是驱动程序导致的。为了保护密码安全，该聊天软件的密码输入框经过了特殊处理，需要

使用特殊的驱动程序对输入的内容进行加密，防范密码盗取软件（没错，虽然这是一个纯粹的软件，但也有驱动，并不是只有硬件设备才需要安装驱动，很多软件为了实现某些特殊的功能，也需要驱动）。然而该软件密码输入框所用的驱动不够完善，不能兼容 Windows Vista，因此，一旦单击密码输入框，系统就会立刻死机。

为了减少驱动程序对系统的影响，早在 Windows 2000 时代，微软就开始对驱动程序实施数字签名机制。简单来说，硬件厂商可以将自己设备的驱动程序提交给微软，由微软在自己的 Windows 硬件质量实验室（Windows Hardware Quality Lab，WHQL）中对驱动的功能、可靠性、安全性等诸多方面进行测试，如果能测试通过，则会给驱动程序添加微软的数字签名，然后直接包含到 Windows 中，或通过 Windows Update 网站提供，另外，也可以由硬件制造商通过自己的网站提供下载。只要驱动程序带有微软的数字签名，就意味着该驱动被微软证实是安全可靠的，不会影响到系统的稳定性和可靠性。不过这项策略在前几年并非是强制的，默认设置的 Windows 中，如果安装不包含微软签名的驱动，Windows 只会提示用户可能存在的风险，并由用户决定要采取怎样的操作。

为了进一步提升可靠性，对于 64 位的 Windows Vista 和 Windows 7，如果要安装内核模式的驱动，必须使用带有微软数字签名的驱动，否则这样的驱动就算安装成功，操作系统也不会加载，因此，这样的驱动并不会进入操作系统内核。虽然带有签名的驱动程序并不意味着是绝对安全的，但至少可以保证带有驱动的恶意软件不会进入到内核，并借此降低系统受到攻击的风险。

强制签名的另一项好处是，可以更清晰地知道某个驱动的来源。为了让自己的驱动获得微软的签名，硬件厂商在提交自己的驱动给微软的同时，还需要提供自己的详细信息，微软会根据这些信息为每个驱动创建标识符。这样，一旦驱动导致系统崩溃或其他问题，通过 Windows 的错误报告机制，微软就可以知道问题具体是由哪个驱动导致的，这个驱动又是谁发布的。在收集了大量这样的信息后，还可以直接将相关内容告诉驱动的作者，由作者改进自己的驱动。

默认情况下，在 64 位 Windows 7 中驱动签名是被强制启用的，并且无法通过常规途径关闭。毕竟这是确保系统可靠和安全的一个重要方式。然而有些时候我们可能也需要安装不包含签名的驱动，例如开发人员在开发驱动的时候，不可能为没有正式发布的驱动添加签名；或者为了使用一个老硬件，不得已只能安装不包含签名的驱动，这种时候又该怎样做？

如果只希望加载未签名驱动程序一次，例如，驱动程序开发人员希望测试自己开发的驱动，可以按照下列步骤操作：

STEP 01 重新启动计算机，在 BIOS 自检之后按下“F8”键，打开如图 1-41 所示的高级启动选项页面。

STEP 02 通过键盘上的方向键，选中“禁用驱动程序签名强制”选项，并按下回车键。

STEP 03 系统会自动启动，并且会加载未经签名的驱动。如果重新启动系统，并使用

正常方式启动，此类驱动将被禁止加载。

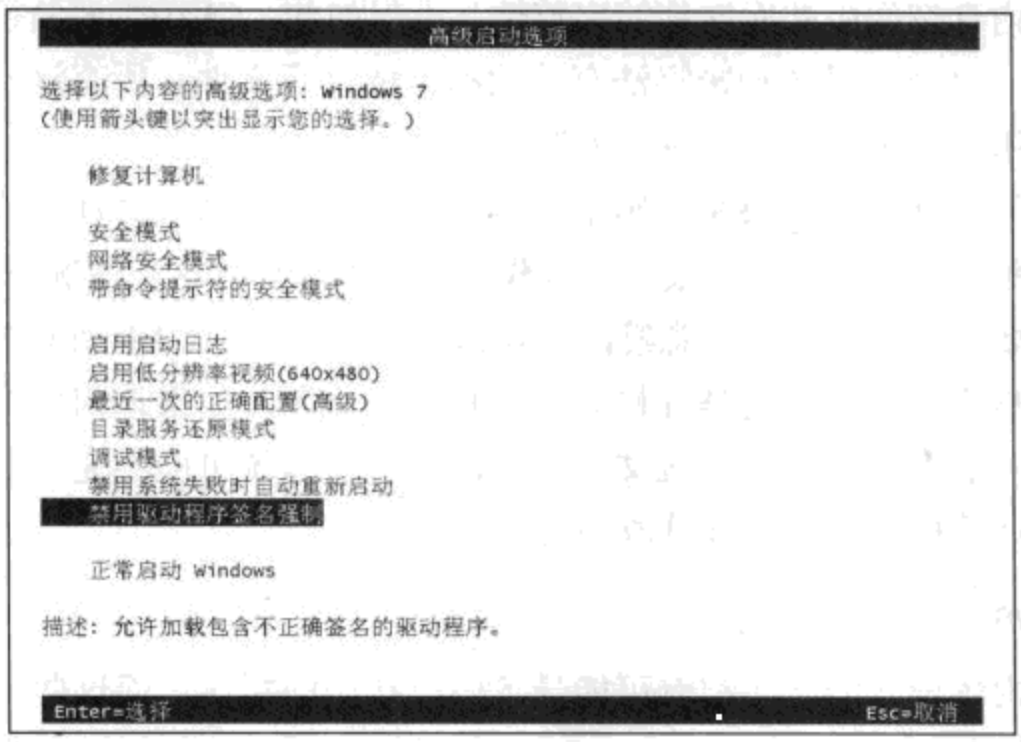


图 1-41　Windows 7 的高级启动选项界面

如果是一般用户，希望在 64 位 Windows 7 中使用驱动未经签名的硬件设备，则需要永久性禁用强制驱动签名，为此，可执行下列操作：

STEP 01 打开“开始”菜单，在搜索框中输入“cmd”，在搜索结果中的“程序 cmd”上单击鼠标右键，选择“以管理员身份运行”，打开管理员权限的命令行窗口。

STEP 02 运行下面两条命令：

```
bcdedit.exe -set loadoptions DISABLE_INTEGRITY_CHECKS
bcdedit.exe -set TESTSIGNING ON
```

STEP 03 重新启动系统，强制驱动签名功能将被彻底禁用。

在经过上述操作之后需要注意，Windows 7 对驱动程序的限制将完全失效，虽然这样可以让老硬件正常使用，但同时也存在着一定的风险。如果希望重新启用强制签名，则可以在管理员身份的命令行窗口中运行下面两条命令：

```
bcdedit.exe -set loadoptions ENABLE_INTEGRITY_CHECKS
bcdedit.exe -set TESTSIGNING OFF
```

1.4.2　更安全的系统内核

除了 64 位 Windows 7 中的安全性改进外，在 Windows 7 中还有很多与安全有关的改进，并且 32 位版本的 Windows 也可以享受到。本节将简要介绍这些内容。

1．代码完整性检查

在 Windows 启动的过程中，代码完整性（Code Integrity，CI）功能会验证系统文件没有被恶意篡改，并确定内核模式中没有运行未经签名的驱动。此时，启动加载程序会检查

内核、硬件抽象层（HAL），以及驱动程序的完整性。在通过验证后，CI 还会检查任何需要被加载到内核内存空间中的库文件的完整性，不仅如此，CI 还需要验证被加载到受保护进程中的库文件，以及与系统加密算法有关的动态链接库文件。所有这一切工作都是自动进行的，不需要用户的干预，也没有可配置的选项。

这样做的目的是什么？如果系统感染了病毒，恶意修改系统文件；或者在计算机关机的情况下遭受了脱机攻击，可能会威胁到操作系统的安全。在这种情况下，通过 CI 的检测可以确保所有重要的文件没有被恶意篡改。Windows 7 中的 CI 可对所有的系统文件，以及内核模式的驱动程序文件进行完整性检查。一旦发现问题，如果该问题存在于驱动中，这样的驱动会被禁止加载；如果是系统文件有问题，整个系统可能会无法启动，此时可以使用安装光盘修复计算机，以替换被篡改的文件。

2. Windows 资源保护

任何运行于内核模式的代码都有可能导致内核数据的损坏，而这些问题的诊断和修复可能非常困难，也非常麻烦。

Windows 7 可以保护系统设置，防范可能导致系统故障或崩溃的错误设置和改动，这个功能叫做 Windows 资源保护（Windows Resource Protection，WRP），它属于老版本 Windows 中文件保护功能的继任者。该功能可以为重要的系统设置、文件，以及文件夹设置非常严格的 NTFS 访问控制列表，防范这些内容被不可信赖的程序修改（管理员用户的修改也将受到限制），这样也可以避免由于无意中改动重要的系统设置导致系统不稳定。

在 Windows 7 中，可以受到 Windows 资源保护功能保护的内容包括：

- 可执行文件、库文件，以及其他 Windows 自带的重要文件。
- 重要的系统文件夹。
- 重要的注册表键设置。

由于该功能的存在，Windows 7 必须安装到 NTFS 文件系统的分区上，因为这样才能对重要的内容设置访问权限。为了证明这一点，可以用鼠标右键单击 Windows 文件夹，选择“属性”，打开“属性”对话框，接着打开“安全”选项卡。从该文件夹的权限设置中即可看到，就算是 Administrators 组的成员，对该文件夹所具有的权限也非常有限，因此，就算恶意代码以管理员身份运行，也无法对重要的系统位置执行可能影响到安全性的操作，进一步保护系统的整体安全性。

该功能没有可配置的选项。

3. Windows 服务加固

以前，很多攻击方式（尤其是蠕虫）都会利用 Windows 服务中存在的漏洞进行网络攻击，这主要是因为很多 Windows 服务都需要监听传入的连接，并且通常具有系统级的特权。因此，一旦出现漏洞，就可以让攻击者通过远程的方式执行高权限任务。

Windows 7 中提供的 Windows 服务加固（Windows Service Hardening）功能对所有的

Windows 服务进行限制，使其只能在文件系统、注册表、网络，或其他可能被恶意软件利用的资源中执行常规的活动，例如，Windows 7 中的远程过程调用（RPC）服务就被限制为只能在预定的端口上进行网络通信，这样就可以排除通过更换系统文件或修改注册表的方式执行恶意操作的可能。Windows 服务加固功能会强制对所有服务的应用所必需的最小特权级别，只为服务分配完成任务所必需的特权。然而 Windows 服务加固功能并不能防范有漏洞的服务被攻陷（这个任务应该由防火墙和自动更新功能实现），只是限制了当一个服务被攻陷后，可能导致的损失和破坏。

Windows 服务加固功能可通过下列手段降低被攻陷服务所造成的影响：

- 为每个服务添加安全标识符（SID），使得不同的服务可被正确区分，并可利用现有的 Windows 访问控制模型对每个服务可访问的对象和资源进行限制。
- 将服务原本使用的 LocalSystem 转为使用特权更少的账户，例如，LocalService 或 NetworkService，这样可以进一步降低服务的权限级别。
- 将每个服务中非必需的 Windows 特权进行严格限制。
- 为服务实施写入限制令牌，使得服务只能访问有限的文件和其他资源，而无法修改系统的其他部分。
- 为服务分配网络防火墙策略，防范服务涉及用途之外的不必要的网络访问，而且这些防火墙策略还可以直接针对每个服务的 SID 进行分配，也可以忽略用户在防火墙中设置的例外或规则。

Windows 服务加固功能的主要目标是降低用户管理服务的工作量，因为 Windows 7 中的每个服务都已经被分配了预定义的 Windows 服务加固配置文件，并且这些配置文件会在 Windows 启动的时候自动应用，完全不需要用户的干预，因此，该功能没有可供配置的选项。

4．地址空间布局随机化

地址空间布局随机化（Address Space Layout Randomization，ASLR）是 Windows 7 中的另一项安全功能，可以让恶意代码更加难以攻破系统。当计算机启动后，ASLR 会将包含操作系统在内的可执行映象（例如.dll 和.exe 文件）随机分配到内存中众多可能的地址位置之一。因此，恶意代码将更加难以确定可执行文件的内存地址位置，也更加难以攻破。

CHAPTER

2

第2章　账户安全

在第1章已经介绍了怎样在Windows中创建用户账户，以及有关用户账户的常用操作。那么到底什么是用户账户，Windows 是通过什么来判断一个用户账户是否具有某些权限的？同时，我们应该怎样做才能保证用户账户的安全？这是本章要讨论的内容。

2.1　用户账户基础

在了解下面的内容之前，首先需要认清一个事实：虽然多用户操作系统（Windows 2000/XP/Vista/7）已经被广泛使用了，不过依然有很多人在像使用单用户操作系统（Windows 9x）那样使用多用户操作系统。当然原因是多种多样的，可能首要原因就是遗留的使用习惯。因为很多人是从 Windows 9x 开始接触 Windows 操作系统，甚至接触计算机的，但随着技术的发展，新操作系统中多用户的特性并未得到足够的重视，导致很多人依然在沿用古老的使用方式。

本节重点介绍多用户操作系统中有关用户账户的一些概念，方便我们能够理解多用户的实现方式，以及在安全上需要注意的问题。

2.1.1　创建用户账户

当我们在 Windows 中创建一个用户账户的时候，都会发生什么事情？首先，系统会根据输入的用户名为该用户创建对应的配置文件（在看过第 1 章有关配置文件的内容后，还记得在 Windows 7 中的用户配置文件都保存在哪里吗？），然后为该账户生成一个唯一的 SID（Security Identifiers，安全标识符），并根据账户的类型给对应的 SID 指派相应的权限或权利，接着将该账户的访问凭据（用户名和密码）等信息加密后保存在数据库中。对于单机和工作组环境下的本地账户，凭据信息保存在本机的 SAM 数据库中；对于域环境下的域全局账户，这些信息保存在域控制器上。在我们给一个对象设置访问权限的时候，实际上是在编辑该对象的 ACL（Access Control List，访问控制列表）。

上述内容涉及了几个概念，下面对这些概念进行解释。

1. 安全标识符

和很多人想象中的不同，Windows 并不是根据每个账户的名称来区分账户的，相反，Windows 依靠的是 SID。在 Windows 环境中，几乎所有的对象都具有对应的 SID，例如本地账户、本地账户组、域账户、域账户组、本地计算机、域、域成员，这些对象都有唯一的 SID（可以将用户名理解为我们每个人的名字，将 SID 理解为每个人的身份证号码，人名可以重复，但身份证号码绝对不会重复）。

这样做主要是为了便于管理，例如，因为 Windows 是通过 SID 区分对象的，我们完全可以在需要的时候更改一个账户的用户名，而不用担心需要对新名称的同一个账户重新设置所需的权限，因为 SID 是不会变化的。同理，如果有一个账户，我们已经给该账户分配了相应的权限，一旦删除了该账户，然后重建一个使用同样用户名和密码的账户，因为账户的 SID 已经发生了变化，因此，尽管账户的名称和密码都相同，但原账户具有的权限和权利并不会自动应用给新账户。

SID 是一个 48 位的字符串，在 Windows 7 中，要想查看当前登录账户的 SID，可以使用管理员身份启动命令提示行窗口，然后运行“*whoami /user*”命令，运行该命令后，我们可以看到类似这样的结果：

```
C:\Windows\system32>whoami /user
用户信息
----------------
用户名      SID
=========== ============================================
Machine\User  S-1-5-21-1859918473-4184378329-583984280-1000
```

该工具可以显示当前登录账户的 SID。如果希望查看本机其他账户的 SID，或者希望在不包含该工具的老版本 Windows 中查看账户 SID，则可以借助微软的一个免费小工具 PsGetSid，该工具可以在 http://tinyurl.com/5tt7fo 中免费下载。使用该工具时，只需要在命令行窗口中输入“PsgetSID”，接着输入一个空格，并输入要查看 SID 的账户名称即可。

虽然 SID 是唯一的，不过依然有一些通用 SID，在 Windows 所有的系统中，这些 SID 都是完全通用的。这些相同的 SID 主要是为了方便管理，例如，表 2-1 列出了一些比较常见的通用 SID。其他常见的通用 SID 请参考微软知识库中的文章：http://support.microsoft.com/ kb/243330。

表 2-1　常见的通用 SID

SID	组	用　途
S-1-1-0	Everyone	用于代表所有用户的组
S-1-2-0	Local	用于代表本地登录的用户
S-1-3-0	Creator Owner	用于代表创建该对象的用户的 SID
S-1-3-1	Creator Group	用于代表创建该对象的用户所在组的 SID

2. 权限和权利

在 Windows 环境下，有两个术语用于表示访问特权：权限（Permission）和权利（Right）。权限是指用某种固定方式访问某个特定对象的能力，例如给 NTFS 分区上写入文件或者删除文件；权利是指执行某些特定操作的能力，例如更改分页文件的设置。

虽然特权分为这两个类别，不过在大部分情况下都没必要过于纠缠这个问题。因此，在很多文章、图书，甚至 Windows 操作系统本身的界面上，特权、权限、权利这三个术语往往都是混用的，本书也是这样。

3. 访问控制列表

为什么我们使用标准账户登录后，无法打开某些关键的系统文件夹？如果需要禁止某个用户打开一个文件夹或文件，此时可通过 NTFS 权限进行限制（有关利用 NTFS 访问权限对文件的访问进行限制的详细信息，请参考本书第 5 章数据安全），其实这些都是访问控制列表（ACL）的功劳。

在 Windows 系统中，每个可访问的对象（文件夹、文件、打印机、计算机等）都有对应的 ACL，为对象设置权限实际上就是在编辑对象的 ACL。举例来说，如果希望禁止用户“User”访问一个文件夹 A，那么实际上就是编辑文件夹 A 的 ACL，在 ACL 中添加拒绝用户“User”（SID）访问的条目。当然，在 ACL 中，用户实际上也是通过对应的 SID 进行区分的。

同理，当一个用户试图访问某个对象时，Windows 的安全子系统首先会根据用户的账户名得到该用户的 SID，然后将 SID 和对象 ACL 中的信息进行对比。如果发现 ACL 中的记录允许该 SID 访问，那么就允许访问；反之，就禁止访问。

2.1.2 登录过程和访问令牌

账户已经创建好了，而且相应的 SID、配置文件，以及权限都设置好了，那么在使用 Windows 的过程中，它们是如何参与到保证系统安全的工作中的？

在登录的时候，如果用户输入的用户名和密码通过了 SAM 数据库或者域控制器的验证，那么 Windows 会自动为该用户生成一个安全访问令牌（Security Access Token），其中包含了这个用户的用户名和 SID 等信息，同时还包含该账户所在用户组的信息（这些内容被统称为安全配置文件）。访问令牌可以看做是一张电子通行证，里面记录了用于访问对象、执行程序，以及修改系统设置所需的安全验证信息。

访问令牌是可以传递的，例如，如果一个用户在登录后试图运行某个程序，那么这个程序就会获得该用户的访问令牌。简而言之，用户运行的程序将具有和用户本身同样的特权。例如，对于管理员用户，他登录后就具有管理员权限的访问令牌，而该用户运行的程序也将具有管理员权限，对系统具有完整的控制权。假设该用户从电子邮件中收到了一个带有病毒的附件，这个病毒会恶意修改系统设置，如果运行该附件，那么这个附件也将具

有管理员权限，因此，完全可以实现修改系统设置的目的；但如果该用户是标准/受限账户，没有修改这个系统设置的权限，那么该用户运行感染病毒的附件后，病毒虽然可以运行，但因为缺少权限，则无法修改系统设置，这也就直接阻止了病毒的破坏。

因此，长久以来，很多安全类的书籍或者文章都会建议大家在 Windows 中创建一个管理员账户，并创建一个标准账户，这样平时可以使用标准账户登录，只有在需要维护系统，或者进行其他需要管理员权限才可以进行的操作时才使用管理员账户登录。

在 Windows 7 中，因为有了全新的用户账户控制功能，该功能可以限制用户的权限，从而进一步保证了系统的安全。

2.1.3　深入理解配置文件

在第 1 章曾简单介绍过 Windows 7 中用户配置文件的一些基本概念，不过很多人可能已经发现，在配置文件夹下还有很多子文件夹和一些快捷方式，这些文件夹分别是做什么用的呢？

用户配置文件夹的层次结构也叫做用户配置文件的名称空间，在 Windows 7 中，名称空间的使用方式与老版本 Windows（主要是 Windows Vista 之前的系统）相比，有较大区别。了解这些区别对于了解最小用户特权这一设计思想是非常重要的，同时名称空间的变化也是第三方应用程序遇到兼容性问题的一个主要原因。因此，下面将以 Windows XP 和 Windows 7 为例，介绍在这两个系统下名称空间的改进。

2.1.3.1　Windows XP 的配置文件名称空间

在 Windows XP（以及更老版本的 Windows）中，用户配置文件名称空间主要有下列特征：

- 本地用户的配置文件位于%SystemDrive%\Documents And Settings 目录下。
- 每个在本机上登录过至少一次的用户都将有一个以自己账户名为名的配置文件夹，也就是“%SystemDrive%\Documents And Settings\用户名”。
- 有一个特殊的配置文件夹%SystemDrive%\Documents And Settings\All Users，其中包含了一些通用的项目，例如，要在所有登录到本机的用户桌面或开始菜单中显示程序的快捷方式，以及桌面图标。通过对该配置文件的内容进行定制，即可让所有登录到本机的用户看到相同的程序快捷方式。
- 有一个特殊的隐藏配置文件夹%SystemDrive%\Documents And Settings\Default User，主要充当为新用户创建配置文件时的模板使用。当用户首次登录到本机时，Windows 会自动加载 Default User 配置文件，并将其复制到“%SystemDrive%\Documents And Settings\用户名”路径下，作为该用户的配置文件。

Windows XP 的配置文件夹内包含的子文件夹主要用于保存应用程序设置和用户数据，其中还有一些文件夹是隐藏的（如图 2-1 所示）。这些重要的文件夹以及用途分别是：

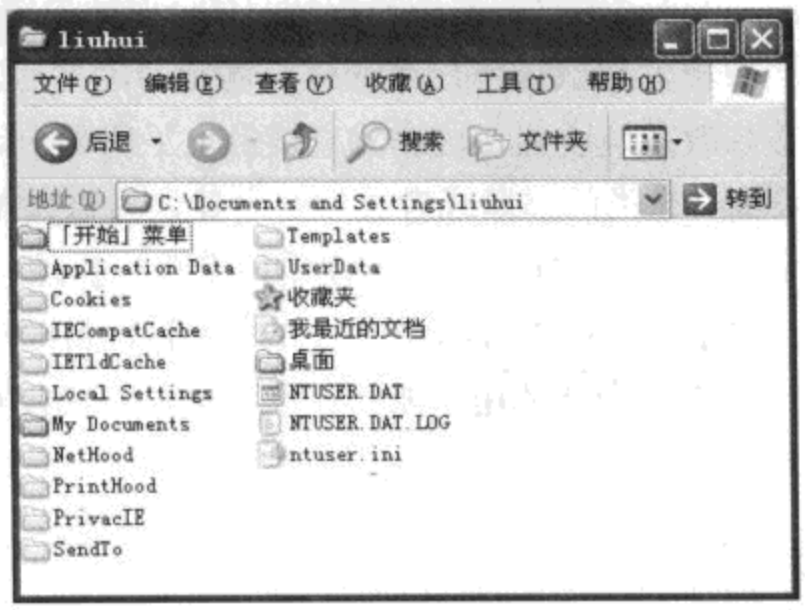


图 2-1　Windows XP 的用户配置文件夹名称空间

- Application Data：包含与特定应用程序有关的数据，例如应用程序的配置参数。
- Cookies：包含 IE 的 Cookie 文件。
- Desktop：包含要在用户桌面上显示的内容，例如文件或快捷方式。
- Favorites：包含 IE 的收藏夹内容。
- Local Settings：包含与特定计算机有关的应用程序设置和数据，或者因为太大不适合在域环境中进行漫游的文件。该文件夹下还有几个重要的子文件夹，包括 Application Data、History、Temp 和 Temporary Internet Files。

窍门　漫游是什么意思？

在域环境中，因为用户可以使用域账户在任何一台加入域的计算机上登录，因此，通过“漫游配置文件”可以将用户的配置文件保存在文件服务器上。这样，用户无论在哪台客户端计算机上登录，都可以直接从文件服务器将配置文件夹下载并缓存到本地，保存在配置文件夹中的内容（例如文档、应用程序的设置等）就可以在任何一台计算机上使用。而用户注销的时候，客户端计算机还会自动将配置文件中修改过的内容重新传输到文件服务器上。

配置文件的漫游只能在域环境中使用，不能用于单机和工作组环境。不过，通过对配置文件重定向，将文件统一保存在网络服务器上也可以获得类似域环境的漫游效果。

- My Documents：用于保存用户所创建的文档的默认位置，也就是“我的文档”。该文件夹还包括几个重要的子文件夹，例如：My Pictures、My Music，以及其他针对特定应用程序的文件夹。
- NetHood：包含要在“网上邻居”中显示的快捷方式。
- PrintHood：包含要在打印机文件夹中显示的快捷方式。

- Recent：包含到最近打开过的文件、程序，以及设置的快捷方式。
- SendTo：包含到不同存储位置以及应用程序的快捷方式，也就是我们熟知的右键“发送到”菜单内容。
- Start Menu：包含要在“开始”菜单中显示的快捷方式。
- Templates：包含用做模板项的快捷方式。

> **注意**　Windows 资源管理器的名称“翻译”功能
>
> 默认情况下，这些文件夹的名称实际上都是英文的，但在中文版 Windows 的资源管理器中打开配置文件夹后会发现，有些文件夹使用了中文的名称，其实这是为了便于使用，Windows 资源管理器所提供的名称“翻译”功能可以自动将一些常用文件夹的名称翻译为更友好的中文。但在文件系统上，这些文件夹依然都使用了英文的名称。

对于 Windows XP 这种用户配置文件夹名称空间，使用起来虽然很方便，但依然存在一定的不足，具体表现在：

- 用户配置文件中同时保存了应用程序和用户数据文件夹，这意味着两种类型的数据会被保存在一起。例如，%SystemDrive%\Documents And Settings \user_name\Local Settings\Application Data 文件夹中就同时保存了针对特定计算机的数据和设置，但这些内容是不能（也不该）被漫游的，而且其中可能会保存过大的不适合漫游的内容，因此，这样的设计并不是很完美。
- My Pictures、My Music，以及 My Videos 等文件夹属于 My Documents 的子文件夹，这些子文件夹中通常会是体积非常大的媒体文件。因此，一旦配置文件夹重定向，在登录和注销时，可能需要通过网络传输大量的数据，这将导致登录和注销时间的延长，而且这种传输往往是不必要的。
- 对于第三方应用程序在配置文件夹的哪些位置存储每个用户的设置和数据，没有统一的约定。例如，有些第三方应用程序可能会在用户配置文件夹下新建子文件夹，用于存储用户信息，而不是使用现有的名称空间位置。而且某些第三方应用程序可能会针对特定计算机的，以及每个用户设置的信息同时保存到 Application Data 文件夹下，这可能会导致某些应用程序漫游后无法使用。

2.1.3.2　Windows 7 的配置文件名称空间

因为存在种种不足，因此，从 Windows Vista 开始，用户配置文件夹的名称空间有了很大变化，Windows 7 也延续了这些变化，这些变化包括：

1）用户配置文件名称空间的根位置从%SystemDrive%\Documents And Settings 移动到%SystemDrive%\Users，这意味着某个用户配置文件夹的位置变为“%SystemDrive%\Users\用户名”，而不再是“%SystemDrive%\Documents And Settings\用户名”。

2）用于保存用户数据的文件夹不再添加“我的”这一前缀，这样在显示上更简洁。但是这里需要再次提醒注意上文曾经提到的 Windows 资源管理器的“翻译”功能，实际上，在 Windows 7 中，配置文件名称空间中的文件夹将不再出现“我的”前缀，但资源管理器在对这些名称进行翻译的时候，依然会添加该前缀（要确认这一点，可以通过 Windows 资源管理器以及命令行窗口浏览配置文件夹的内容）。

3）Windows 7 中的 My Music、My Pictures，以及 My Videos 文件夹不再是 My Documents 的子文件夹，并且这些文件夹开始直接保存在配置文件夹的根路径下，与 My Documents 文件夹的层次结构是相等的。通过这样的设置，用户自己的数据以及应用程序设置之间可以更好地分开。

4）在配置文件夹根目录下，新增了多个子文件夹，以便更方便地保存不同类型的用户数据和设置，新增的子文件夹包括以下 5 个。

- Contacts：用于保存用户联系人信息的默认位置。
- Downloads：用于保存所有下载文件的默认位置。
- Searches：用于保存已保存搜索（也就是虚拟文件夹）的默认位置。
- Links：用于保存 Windows 资源管理器收藏夹内容的默认位置。
- Saved Games：用于保存游戏存盘记录的默认位置。

5）为了让应用程序更好地实现漫游，在 AppData 文件夹下新建了三个相互分离的子文件夹，其作用分别为：

- **Local** 该文件夹保存了无法（也不该）被漫游的与计算机相关的应用程序数据和设置，以及因为太大而无法有效漫游的用户自己的数据或设置。Windows 7 中的 AppData\Local 文件夹实际上等同于老版本 Windows 中的 Local Settings\Application Data 文件夹。
- **Roaming** 该文件夹保存了应当（或者必须）被漫游的与用户相关的应用程序数据和设置，Windows 7 中的 AppData\Roaming 文件夹实际上等同于老版本 Windows 中的配置文件夹根目录下的 Application Data 文件夹。
- **LocalLow** 该文件夹可供低完整性进程获得写操作的权限。低完整性进程执行的操作不能影响操作系统，例如，由保护模式下的 IE 所启动的应用程序就只能使用该配置文件夹存储应用程序的数据和设置。LocalLow 文件夹是 Windows Vista/7 中新增的。

6）All Users 配置文件被更名为 Public，这样可以更好地凸显其用途。保存在该文件夹下所有的内容都可被本机的所有用户使用，而该文件夹的某些子文件夹（例如 Desktop 的内容）则会在用户登录到本机后，合并到该用户自己的配置文件夹中。

7）Default User 配置文件被更名为 Default，与 Windows XP 中的 Default User 类似，Windows 7 中的 Default 配置文件是从不被加载的，只会在新建配置文件的时候直接复制。因此，也是作为用户首次登录本机时创建配置文件的模板使用。

2.2　用户账户控制（UAC）

用户账户控制（UAC）功能最早出现在 Windows Vista 中，在 Windows 7 中，微软对 UAC 功能进行了大量改进，在确保安全性的同时，让 UAC 的提升提示出现的数量更少，而且我们可以根据需要使用不同级别的提示，因此，在确保安全的同时，也进一步提升了易用性。

虽然很多有关安全的文章一直都在建议平时使用标准账户的权限登录系统，并执行各种操作，只有在需要执行管理任务的时候才使用管理员账户。但实际上，在 Windows Vista 发布之前的时代，如果想要在日常操作中使用非管理员账户实现常规操作，往往是很困难的，这主要是因为：

- 很多应用程序只有在提供管理员特权的情况下才能运行，哪怕本身可能只是一个非常简单的小游戏。
- 如果希望使用低特权运行应用程序，往往需要使用 Runas 命令，这样非常不方便。
- Windows 自身的一些操作，例如更改时区、添加打印机等，也需要管理员特权。

Windows Vista/7 中的 UAC 功能则能让不具备管理员特权的账户在使用上更方便，这些方便具体体现在：

- **大部分应用程序可以在没有管理员特权的情况下正常运行**。针对 Windows 7 设计的应用程序并不会要求无谓的管理员特权，而且 UAC 会通过下文将要介绍的文件系统和注册表虚拟化技术为存在问题的程序提供向后兼容性。
- **要求管理员特权的应用程序会在必要时向用户显示提升提示**。例如，在修改某些应用程序的配置时，如果修改的是只影响当前用户的选项，那么可以直接修改；如果被修改的是影响整机所有的用户，甚至影响系统本身的设置，那么在应用这些改动的时候就需要经过提升提示。
- **执行常规任务不再要求管理员特权**。Windows 7 中包含大量的改进，这样标准用户即可在不需要提供管理员凭据的情况下执行大部分常规的配置工作。例如，在老版本 Windows 中，只有管理员可以更改时区，而在 Windows 7 中，普通用户即可修改，对于需要跨国旅游的人来说，这是非常方便的改进。但由于更改系统时钟可能产生较大的影响，因此，在 Windows 7 中，依然只有管理员可以修改系统时钟。
- **对于需要管理员特权的功能，操作系统会使用盾牌图标标识出来**。在老版本 Windows 中，用户可能根本不知道操作系统的哪些功能要求使用管理员特权，只有在真正进行修改时才会遇到错误信息。但在 Windows 7 中，任何需要管理员特权的内容都会用醒目的盾牌图标标识出来。
- **就算使用管理员账户登录，Windows 7 依然默认使用标准用户的权限运行应用程序**。虽然建议大部分用户平时使用标准账户登录系统，但也会有人习惯于使用管理员账

户登录。有了 UAC 的保护后，用户执行的程序依然会使用标准用户的特权，这样做无疑更加安全。

因为在特权的使用上有了较多的改变，因此，相比 Windows XP，带有 UAC 的 Windows Vista/7 在某些方面的行为也出现了不同，它们的区别如表 2-2 所示。

表 2-2 Windows XP 与带有 UAC 的 Windows 7 的区别

Windows XP	使用 UAC 的 Windows 7
作为标准用户登录后，管理员可以用鼠标右键单击程序，选择“运行方式”，然后提供管理员凭据	标准用户不需用鼠标右键单击，即可打开需要高权限的工具，UAC 随后会要求用户提供凭据。所有的用户也可以用鼠标右键单击的方式用管理员凭据启动程序
标准用户账户几乎无法使用，尤其是技术型用户或移动用户	标准账户可执行以往需要管理员权限的大部分普通操作，在需要时，Windows 7 会询问管理员凭据
如果用户使用标准账户登录，应用程序一旦试图更改受保护位置的文件或设置，将会直接失败	如果用户使用标准账户登录，UAC 会对系统的重要位置进行虚拟化重定向，这样即可在保护操作系统完整性的同时让应用程序正常运行
如果特定的 Windows 功能需要管理员特权，则整个工具都需要提供管理员特权	Windows 7 会使用 UAC 的盾牌图标提示用户该功能要求管理员特权
如果用户使用管理员账户登录，运行的所有的应用程序都将具有管理员特权	如果用户使用管理员账户登录，所有的应用程序依然以标准用户的权限运行。如果要启动非 Windows 自带的要求管理员特权的软件，需要进行 UAC 提升，要求管理员特权的 Windows 自带工具可以不经提示，自动获得所需的权限

UAC 是一个有用的功能，可因为一些误解，使得该功能受到了不少质疑。例如，很多人觉得这个功能对系统安全不仅起不到任何提高作用，反而增加了使用的难度，因为很多老程序在该功能面前遇到了兼容性问题，同时该功能也令很多操作更加烦琐。

本节会介绍有关 UAC 的相关知识，相信通过阅读本章的内容后，我们对 UAC 的了解将会加深，同时更能根据自己的实际情况判断 UAC 是否是鸡肋，是否应该禁用。

2.2.1 什么是 UAC

和老版本的 Windows 有很大不同，在 Windows 7 中，当用户使用管理员账户登录时，Windows 会为该账户创建两个访问令牌：一个标准令牌，一个管理员令牌。大部分时候，当用户试图访问文件或运行程序的时候，系统都会自动使用标准令牌进行，只有在权限不足（也就是说，如果程序宣称需要管理员权限的时候）时，系统才会使用管理员令牌；如果程序没有宣称自己需要管理员权限，此时程序的部分功能可能无法正常使用，或者程序无法运行，这也是在启用 UAC 的情况下，某些应用程序兼容性问题的主要原因。

这种将管理员权限区分对待的机制叫做 UAC（User Account Control，用户账户控制）。简单来说，UAC 实际上是一种特殊的“缩减特权”运行模式。

在进行需要管理员特权的操作时，系统首先会弹出“UAC”对话框要求用户确认（如

果当前登录的是管理员用户），或者输入管理员用户的密码（如果当前登录的是标准用户）。只有在提供了正确的登录凭据后，系统才允许使用管理员令牌访问文件或运行程序。这个要求确认或者输入管理员账户密码的过程叫做“提升”。

根据账户类型的不同，在 Windows 7 中有两种不同的“提升”对话框。如果当前登录的是管理员账户，那么“提升”对话框将如图 2-2 所示，只需确认即可继续；如果当前登录的是标准账户，那么“提升”对话框将如图 2-3 所示，此时需要输入一个管理员账户的密码才能继续。

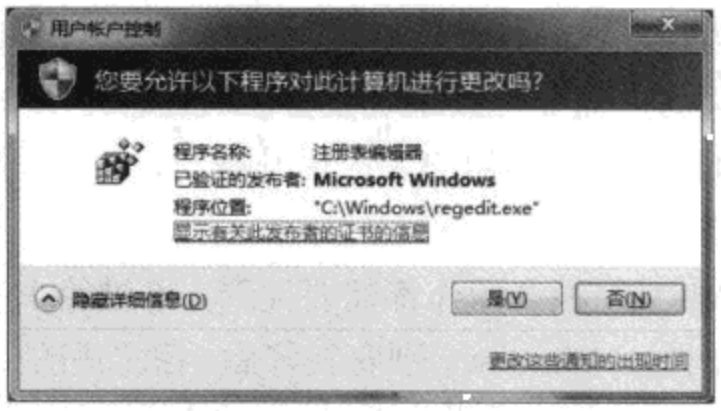


图 2-2　管理员账户的“提升”对话框

图 2-3　标准账户的“提升”对话框

在管理员账户的“提升”对话框中，可以看见当前要使用管理员全新安装运行的程序的名称，单击“详细信息”按钮后可以看到该程序的安装路径等信息。而根据实际情况，如果希望运行该程序，可以单击“继续”按钮，否则可以单击“取消”按钮。

在标准账户的“提升”对话框中，除了上述内容外，主要还显示了当前本机上的所有管理员账户，此时需要选择一个管理员账户，然后输入密码，即可单击“继续”按钮运行该程序。

另外，取决于要以管理员身份运行的程序的不同，“提升”对话框顶部一栏的底色可能会有所变化，一般来说，我们可以见到的底色以及对应的含义如下：

- **红色背景，带有红色盾牌图标**　表示该程序的发布者被禁止，或者被组策略禁止。在遇到这种“提升”对话框的时候要万分小心。
- **橘黄色背景，带有红色盾牌图标**　表示该程序不被本地计算机信任（主要是因为不包含可信任的数字签名或者数字签名损坏）。
- **蓝绿色背景**　表示该程序是 Windows Vista 自带的程序（带有微软的数字签名）。
- **灰色背景**　表示该程序带有签名并且被本地计算机信任（带有可信任的数字签名）。

在 Windows 7 中，很多选项旁都被增加了一个彩色的盾牌图标（如图 2-4 所示），这个图标表示该选项需要更高的权限，使用之前首先要经过 UAC 的提升。

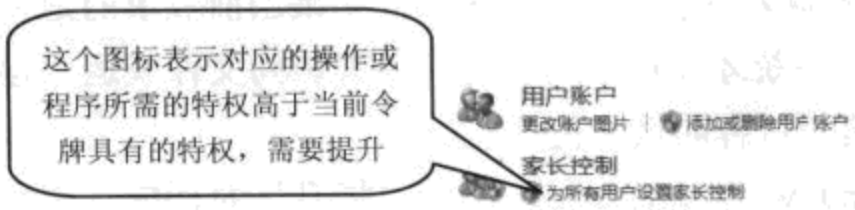


图 2-4　需要提升后才能运行的选项

2.2.2　配置 UAC

很多对 UAC 抱有成见的人主要分为两种情况。

新手往往认为，UAC 功能让原本就显得有些烦琐的操作变得更加烦琐，因为在执行很多操作的时候都需要进行确认，或者输入管理员密码。

对 UAC 以及对系统安全有所了解的人则认为，UAC 虽然可以对恶意软件的运行制造人为的障碍，但并不能彻底解决问题。例如，如果病毒需要修改系统设置，或者破坏系统，而反病毒软件因为各种原因没能及时拦截，虽然 UAC 会要求用户完成提升操作，但如果用户对此不够了解，随随便便就单击了“继续”按钮，那么病毒依然会成功运行。

其实这两种看法都很好理解。确实，启用 UAC 后，很多操作都需要提升，不过绝大部分操作都是可以在不需要提升的情况下进行的。例如，Windows 刚安装好后，我们可能需要根据实际情况对一些系统设置进行调整，在这个过程中可能会经常被 UAC 打断。然而，一旦配置好系统，在平时的使用中，绝大部分人很少，甚至完全不需要对重要的系统选项进行其他调整。因此， UAC 的存在与否在这时候已经不再那么“扰民”了。

至于应用程序，很多程序因为其特殊性，例如需要直接读写关键的系统文件，或者需要工作在系统底层，每次运行的时候都需要提升。但这往往是少数情况，随着 Windows Vista/7 等包含 UAC 功能的 Windows 操作系统的进一步普及，应用程序开发商针对 UAC 开发出兼容性更好的程序后，这种现象也会越来越少。

至于很多人认为的如果不了解整个机制的人在遇到 UAC“提升”对话框后随随便便单击“继续”按钮，这确实是存在的。然而安全性最薄弱的环节永远在用户，毕竟操作系统不能直接对用户的操作进行干预。例如，如果用户要执行某个病毒文件，操作系统根本无法判断用户到底是无意中执行的，还是因为要研究这个病毒而故意执行的，因此，Windows 只能用“提升”对话框告诉用户执行这个操作需要较高的权限才能进行，需要谨慎，至于是否接受操作系统的建议，是否继续进行这个操作，这依然取决于用户本身。

从另一方面考虑，这个提升过程还是可以增强系统安全性的。例如，从网上下载了一个软件的安装程序，该安装程序中被捆绑了病毒，但我们并不知道这件事，那么在运行这个软件的时候，因为我们知道这个软件是公司 A 开发的，带有公司 A 的数字签名，但 Windows 突然显示了一个“提升”对话框，告诉我们有个未经签名的或者由公司 B 签名的软件需要管理员权限才可以安装，这时候相信对 UAC 的工作原理有所了解的人都会意识到其中存在的问题。

在 Windows 7 的默认设置中，UAC 的很多行为经过改进和调整后，已经不再那么烦人。而且通过选项还可以修改 UAC 的提示级别。因此，下文将介绍如何让 UAC 在确保系统安全的同时，能够更加安静。

2.2.2.1　修改默认提示级别

如果认为 Windows 7 中默认设置的 UAC 依然比较烦人，那么可以通过下列操作调整提示级别：

STEP 01 使用管理员账户登录 Windows 7，打开“控制面板”。

STEP 02 在“控制面板”中依次单击“用户账户和家庭安全”→“用户账户”→“更改用户账户控制设置”。

STEP 03 在随后出现的如图 2-5 所示的界面中，可通过滑块调整 UAC 的提示级别。这里提供了五个级别，从上到下的安全性递减，同时，“扰民”的程度也是递减的。

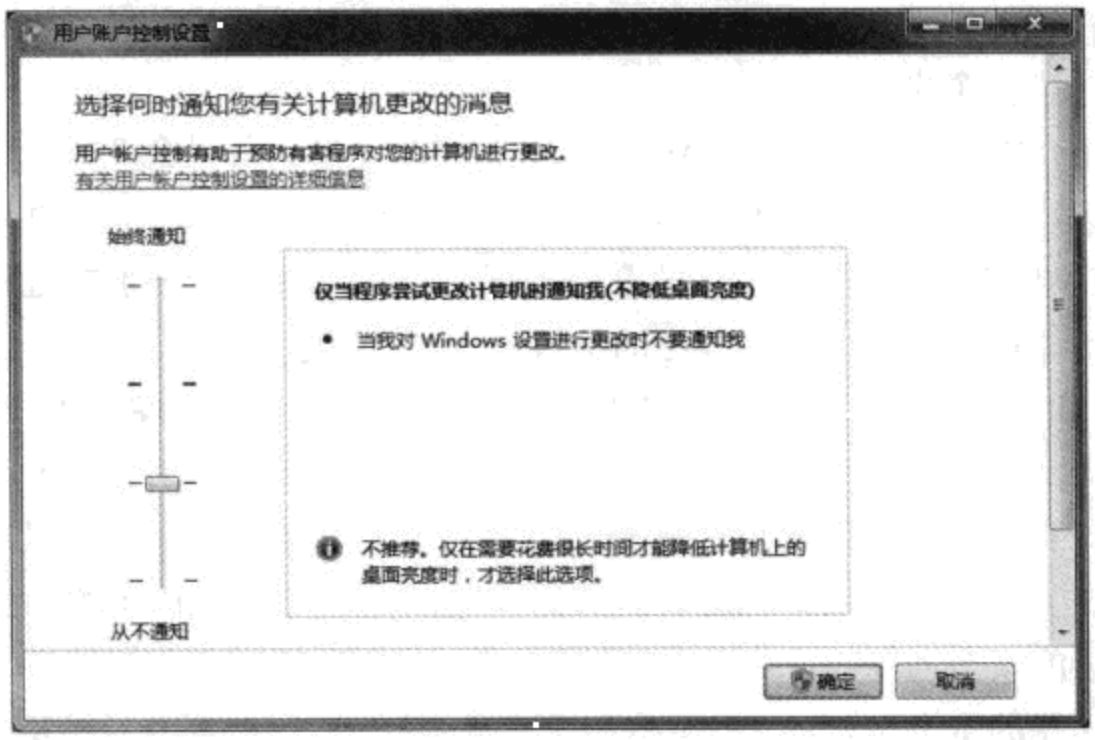


图 2-5　更改 Windows 7 的 UAC 提示级别

STEP 04 如果希望彻底将 UAC 的提示关闭，则可以将滑块拖动到最底部。但是这并不是禁用了 UAC，只不过 UAC 不再显示任何提示信息而已。

STEP 05 单击“应用”按钮，此时取决于具体的设置，可能需要重新启动系统，其中的修改才能生效。

上述不同级别之间的区别，以及建议的使用环境可参考表 2-3。

表 2-3　Windows 7 UAC 提示级别及使用环境

选　项	描　述	适 用 场 景	是否使用安全桌面
始终通知	当程序试图安装软件，或更改计算机设置，或用户更改 Windows 设置时，通知当前用户	如果希望尽可能保证计算机安全，用户需要频繁安装软件，以及访问不熟悉的网站时，可使用该选项	是

续表

选　项	描　述	适 用 场 景	是否使用安全桌面
默认值	只有在程序试图修改计算机配置时通知当前用户，但用户自己更改 Windows 设置时不通知	如果计算机需要较高的安全等级，并希望降低用户可以看到的通知数量时，可选择该选项	是
仅当程序尝试更改计算机时通知我（不降低桌面亮度）	与默认值相同，但显示通知时 UAC 不切换到安全桌面	如果用户在可信赖环境中工作，只使用熟悉的应用程序，不访问不熟悉的网站，即可选择该选项	否
从不通知	关闭 UAC 所有的提示通知	如果安全性并不是最重要的，并且用户在可信赖环境中工作，同时使用由于不支持 UAC 而无法获得 Windows 7 认证的程序，即可使用该选项	否

对于普通用户，通常情况建议将默认的（第三）级别下调一个级别，这样可以获得与默认设置完全相同的安全保护，只不过在显示 UAC 提升对话框的时候，整个屏幕不再变暗，这也就是所谓的“安全桌面”。

默认情况下，Windows 7 弹出 UAC 提升对话框时，桌面背景会变暗。这样做的主要原因并不是为了突出显示 UAC 的对话框，而是为了安全。由于 UAC 对话框运行在安全桌面上，所以安全性非常好。除了受信任的系统进程之外，任何用户级别的进程都无法在安全桌面上运行。这样就可以阻止恶意程序的仿冒攻击。

举例来说，如果有恶意软件打算伪造 UAC 的提升对话框，以便骗取用户的账户和密码，如果没有安全桌面功能，那么用户如果没能区分出真正的 UAC 提升对话框，或者伪造的对话框太过逼真，那就有可能泄露自己的密码。而使用安全桌面功能后，因为真正的提升对话框都是显示在安全桌面上的，而这种情况下，用户无法和其他程序的界面进行交互，因此，避免了大量的安全问题。

安全桌面功能的本意是好的，但有些情况下可能会比 UAC 提升对话框本身更烦人。例如，在切换到安全桌面时，整个屏幕首先会黑一下，然后桌面上显示的其他内容都被变暗显示，并且这些内容都无法操作。实际上，在屏幕变黑的过程中，系统会自动给整个桌面截图，然后全屏显示到安全桌面上作为背景，并在这个背景之上显示提升对话框。对于某些计算机，如果性能不够强，或者驱动有问题，就可能导致这个过程的速度缓慢，影响正常操作。因此，如果不能忍受安全桌面功能，可以考虑将 UAC 的提示下调一个级别。

2.2.2.2　用策略控制 UAC

在按照本节的内容操作之前需要注意，本节需要调整组策略设置，然而只有 Windows 7 商业版/企业版/旗舰版才具有组策略功能。家庭基础版和家庭高级版 Windows 7 不带有组策略功能。

打开“开始”菜单，在“搜索”对话框中输入“secpol.msc”后按回车键，打开本地安全策略控制台。在窗口左侧的控制台树中依次定位到“安全设置”→“本地策略”→“安

全选项”，随后在右侧窗格中可以找到 10 个以“用户账户控制”字样开头的策略（如图 2-6 所示）。本节要介绍的就是这 10 条策略（关于其他策略的详细信息，请参考本书第 3 章策略安全）。

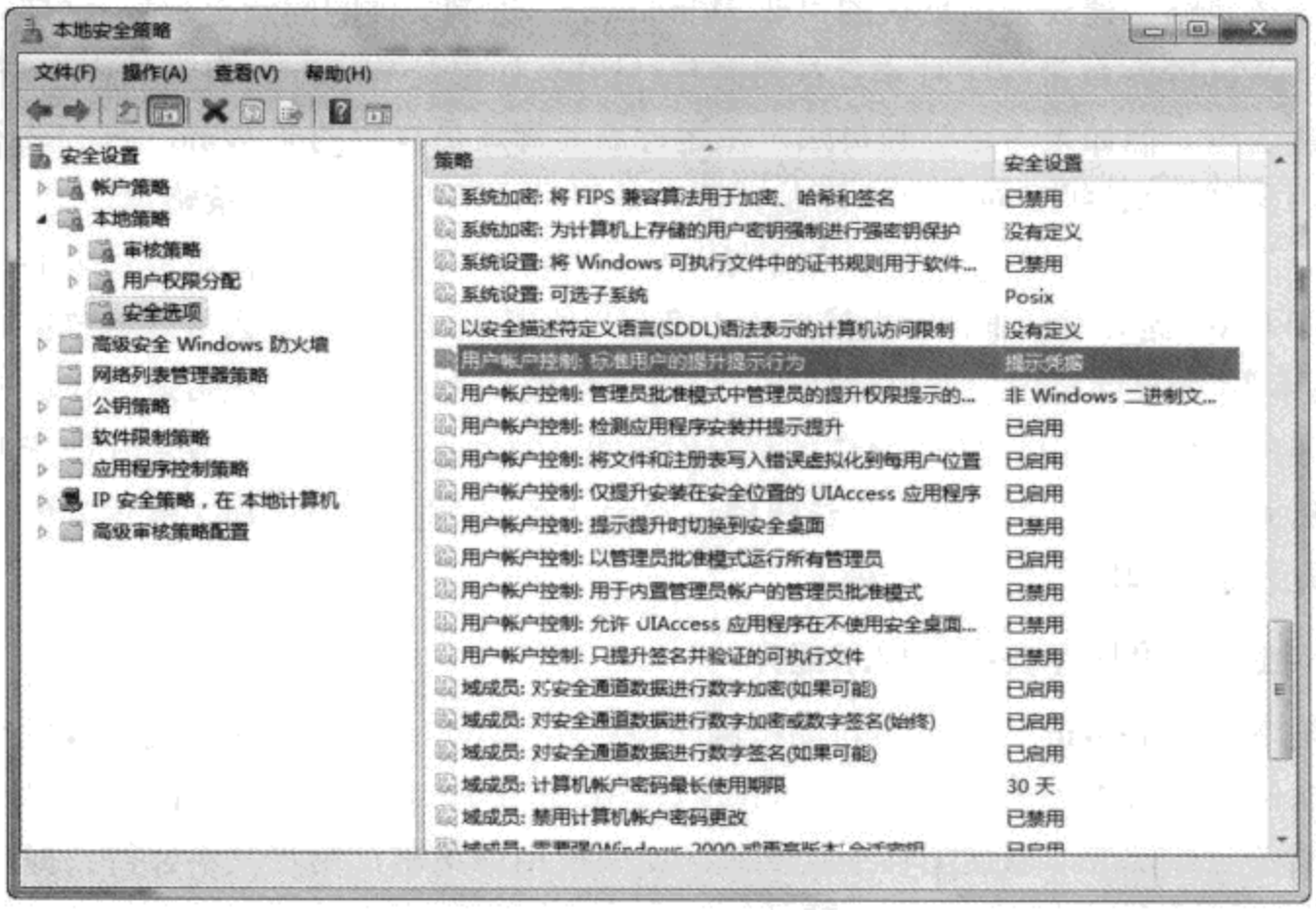


图 2-6　用于调整 UAC 行为的 10 条策略

1. 标准用户的提升提示行为

该策略决定了使用标准用户账户登录的用户在运行需要管理员权限的程序时，是否可以看见提升对话框。默认情况下，使用标准账户登录的用户在运行需要管理员权限的程序时，会被要求输入管理员账户的登录凭据（也就是密码），但通过配置这个选项，用户就不会看到提示。在这种情况下，用户将无法通过提供管理员账户登录凭据的方式获得提升后的权限，也就无法继续进行操作。但该设置并不能阻止用户用鼠标右键单击程序的快捷方式，然后选择“以管理员身份运行”的方式进行提升。

如果希望标准用户在需要时可以看到 UAC 提升对话框，那么可将该策略设置为“提示凭据”，同时这也是默认设置。如果不希望标准用户在需要的时候看到 UAC 提升对话框，可以将该策略设置为“自动拒绝提升请求”。

2. 管理员批准模式中管理员的提升提示行为

该策略决定了受限于管理员批准模式的管理员账户在运行需要管理员权限的程序时，是否可以看到提升提示，同时还决定了提升提示的工作方式。默认情况下，管理员在运行需要管理员权限程序时会被要求批准，但只要单击“继续”按钮，不用输入自己的密码，就可以完成提升操作。如果配置了该选项，那么管理员也必须输入自己的密码，就好像标准用

户做的那样。我们还可以通过配置这个选项让管理员看不到任何提示，这种情况下，管理员也将无法提升自己的特权。不过这样做并不能防止管理员用鼠标右键单击一个程序的快捷方式，然后选择“以管理员身份运行”。注意，该策略不影响系统内建的 Administrator 账户。

对于该策略，建议使用默认的“非 Windows 二进制文件的同意提示”，这样只有在需要提升非 Windows 自带程序时才会看到提升对话框，如果是 Windows 自带的程序需要提升，则可直接通过。但如果希望管理员账户在运行需要管理员权限的非 Windows 自带程序时，可以不用见到 UAC 提升对话框，而是直接自动提升，那么可以将该策略设置为“不提示，直接提升”（通常不建议这样做）。如果希望管理员账户在运行需要管理员权限的程序时，可以看到 UAC 提升对话框，但直接单击“确定”按钮即可继续，那么可以将该策略设置为“同意提示”（如果计算机只有自己使用，可以这样做）。如果希望管理员账户在运行需要管理员权限的程序时，可以看到 UAC 的提升对话框，同时必须输入自己或者其他管理员账户的密码后才可以继续，那么可以将该策略设置为“提示凭据”（如果别人偶尔需要使用我们自己的账户运行程序，建议这样做）。

3. 检测应用程序安装并提示提升

该策略决定了 Windows 是否自动检测应用程序的安装，并提示权限提升或批准。因为该策略默认是启用的，Windows 会自动检测应用程序的安装，并在需要的时候提示用户提升权限或者进行批准，以便能够继续安装。如果禁用该策略，用户就不会得到提示，在这种情况下，用户将无法通过提供管理员凭据的方式提升权限。

也就是说，如果希望 UAC 功能在自动检测到安装程序的运行时自动提升权限，提示用户单击“继续”按钮或者“允许”按钮，或者输入管理员账户密码，那么可以将该策略设置为“已启用”；如果希望 UAC 功能在自动检测到安装程序的运行时不提升权限，而是彻底禁止用户安装需要提升后才可以安装的程序，那么可以将该策略设置为“已禁用”。这样做并不会禁止少数不需要提升且使用标准权限即可安装的程序的正常安装。而且如果直接在安装文件的图标上单击鼠标右键，选择“以管理员身份运行”，也可以直接提示并进行安装，此时不会受到该策略的影响。

4. 将文件和注册表写入错误指定到每个用户的位置

该策略决定了是否打开文件和注册表的虚拟化功能。因为该策略默认是启用的，因此，与虚拟化文件，以及注册表键有关的错误提示和错误日志会被写入到虚拟位置，而不是程序试图写入的实际位置。如果禁用该策略，当应用程序试图写入受保护的文件夹或注册表键的时候，就算出现错误，也不会得到提示。

> **注意** 禁用该策略有可能导致一些老的不兼容 Windows 7 的应用程序无法正常运行，同时因为这条策略对一般用户的交互使用影响不大。为了安全、稳妥起见，最好不要修改该策略的默认设置。

5. 仅提升安装在安全位置的 UIAccess 应用程序

该策略决定了是否只有安装在文件系统中安全位置下的 UIAccess 程序才能被提升。如果启用该策略，只有位于%SystemRoot%\Program Files、%SystemRoot%\Program Files(x86)，或%SystemRoot%\Windows\System32 下的 UIAccess 程序才会受到影响。

窍门　什么是 UIAccess 程序？

UIAccess 是一种用于提升软件可用性的技术，但因为 UAC 的某些设计特性，可能会在使用中导致一些问题。例如，盲人在使用计算机时，通常需要使用读屏软件（也就是一种 UIAccess 程序）将屏幕上显示的菜单、对话框等内容转变成声音，这样才能正确操作计算机。然而在启用安全桌面的情况下，读屏软件将无法与安全桌面的内容进行交互，也就无法读取安全桌面中提升对话框的内容，这会对盲人用户的使用造成不便。因此，在 UAC 的设计过程中，就考虑到了这些特殊情况，并允许对这类辅助软件进行提升，协助用户的正常使用。

该策略会影响到 Windows 的完整性级别检查，同时对普通用户的交互影响不大，因此，建议保持默认设置，不要更改。当然，该策略只有在使用安全桌面的情况下才有意义，如果已经禁用了安全桌面，可以忽略该策略。

6. 提示提升时切换到安全桌面

该策略决定了 Windows 7 在显示提升提示的时候是否切换到安全桌面。安全桌面可以将该程序和进程限制在桌面环境上，这样可以降低恶意软件或用户可以访问需要提升的进程的可能性。默认情况下，这个安全选项是被启用的，如果不希望 Windows 在提示提升之前切换到安全桌面，那么可以禁用该策略。然而这可能使得计算机更容易被恶意软件所感染和攻击。当然，对于安全桌面，更简单的方法是使用上文介绍的内容，将默认的 UAC 提示下调一个级别。

7. 以管理员批准模式运行所有的管理员

该策略决定了使用管理员账户登录的用户是否使用管理员批准模式。默认情况下，这个策略是启用的，这也就意味着管理员也是以管理员批准模式运行，因此，管理员批准模式下的管理员账户也会在适当的时候遇到提升提示。如果禁用了这个设置，使用管理员账户登录的用户不受管理员批准的影响，也不会看到提升提示。

简单来说，如果启用该策略，可以对管理员账户启用 UAC 功能；如果禁用该策略，那么对管理员账户的 UAC 功能也会被禁用（对标准用户的 UAC 依然会启用）。

8. 用于内置管理员账户的管理员批准模式

该策略决定了使用系统内建的 Administrator 账户登录的用户和进程是否受限于 UAC。

默认情况下，该策略是启用的，这意味着内建 Administrator 账户也受限于 UAC，同时还受限于针对管理员账户的提升提示行为设置。如果禁用该设置，使用内建 Administrator 账户的用户和进程将无法受限于管理员批准模式，因此，也不受限于针对管理员账户的提升提示行为设置。

简单来说，如果希望内建 Administrator 账户也受制于 UAC 的限制，那么可以将该策略设置为“已启用”；如果希望内建 Administrator 账户不受 UAC 的限制，可以将该策略设置为“已禁用”。

9. 允许 UIAccess 应用程序在不使用安全桌面的情况下提升权限

上文已经介绍了 UIAccess 程序的用途，并且可以通过上文介绍的策略同时提升此类程序。然而这就遇到了一个新问题，UIAccess 程序在提升之前，无法与安全桌面进行交互，但对 UIAccess 程序进行提升的时候，还是需要出现安全桌面，这依然会造成不便。

因此，通过启用该策略可以在确保其他所有的程序都在安全桌面上提升的同时，让 UIAccess 程序的提升不通过安全桌面进行。当然，该策略只有在使用安全桌面的情况下才有意义，如果已经禁用了安全桌面，可以忽略该策略。

10. 只提升签名并验证的可执行文件

该策略决定了系统对待不同类型的可执行文件的方式。如果希望禁止用户运行未经签名的或者未经验证的可执行文件，那么可以将该策略设置为“已启用”；如果不想禁止用户运行未经签名的或者未验证的可执行文件，则可以将该策略设置为“已禁用”，这也是 Windows 7 的默认设置。

2.2.2.3 UAC 的高级设置技巧

通过上述几个策略的调整，相信 UAC 已经顺眼不少了。但对于使用不带组策略功能的 Windows 7 的读者，或者通过调整策略依然觉得不满意的读者，可以试试使用下文介绍的几个技巧。

1. 临时绕过 UAC

有时候，我们可能要面临这样的问题：需要在短时间内调整大量的系统设置（例如，Windows 刚安装好后的配置阶段），但每次都通过 UAC 的提升显得有些多余。这时候，很多人可能会觉得应该先临时禁用 UAC，等所有的设置都修改完之后再将其启用。可这存在一些不足：启用和禁用 UAC 都需要重新启动系统才能生效，这样显得效率很低。另外，如果在禁用 UAC 后还需要运行 Internet Explorer 查阅资料，因为没有了 UAC 的保护，网页中如果包含恶意代码，很可能会危及系统安全。

其实有更好的办法，不用禁用 UAC，也不用重新启动系统，一样可以临时绕过 UAC，具体操作如下：

STEP 01 在 Windows 的任务栏空白处单击鼠标右键，选择“任务管理器”，打开任务

管理器。

STEP 02 切换到“进程”选项卡，在“Explorer.exe”进程上单击鼠标右键，选择“结束进程”。这样，Windows 任务栏、桌面图标，以及所有打开的资源管理器窗口都会消失。

STEP 03 依然是在任务管理器的“进程”选项卡下，单击“显示所有用户的进程”按钮，并接受 UAC 提升提示。

STEP 04 在任务管理器窗口的“文件”菜单下单击“新建任务（运行）”命令，并在随后出现的“创建新任务”对话框中输入“explorer”后按回车键。

STEP 05 接下来，Windows 任务栏以及桌面图标会重新出现。在这种情况下，通过控制面板或者其他方式执行的程序或者选项不需要提升，直接就具有管理员权限。

这是一个很方便的技巧，它实现的原理是什么？在介绍之前，首先需要明白两个概念：父进程、子进程。顾名思义，如果一个程序 A 启动了另外一个程序 B，那么这两个程序就是父子关系，其中程序 A 是程序 B 的父进程，而程序 B 是程序 A 的子进程。举一个更形象的例子吧，如果运行 cmd.exe，打开命令提示行窗口，然后在命令提示行窗口中执行一个命令行程序，例如 ping.exe，这时候 cmd.exe 就是 ping.exe 的父进程，而 ping.exe 就是 cmd.exe 的子进程。

在启用 UAC 的情况下，当用户登录 Windows 的时候，Windows 首先会用标准令牌启动 explorer.exe，该进程就是俗称的 Windows 外壳，也可以理解为初始进程（其他所有用户进程的父进程），同时我们看到的 Windows 任务栏、桌面图标、“开始”菜单都是由 Windows 外壳产生的。而在登录后，如果需要通过“控制面板”设置某个系统选项，因为“控制面板”也是 Windows 外壳的一部分，又因为 Windows 外壳是使用标准令牌启用的，因此，“控制面板”中的选项（Windows 外壳的子进程）也会使用标准令牌启动，而因为权限不足，我们就会看到 UAC 提升对话框。

在上文中的 **STEP 03** 中，因为单击了“显示所有用户的进程”按钮，这个按钮会提升任务管理器，使其具有管理员权限。在 **STEP 04** 中通过 Windows 任务管理器运行的 Windows 外壳就成了具有管理员权限的任务管理器的子进程，进而得到了一个具有管理员权限的 Windows 外壳。那么在提升了权限的 Windows 外壳上修改其他系统选项的时候，自然也就不需要额外的提升了。

如果修改完设置需要重新打开标准权限的 Windows 外壳，又该怎么办？可以进行下列操作：

STEP 01 在任务栏空白处单击鼠标右键，选择“任务管理器”，打开任务管理器窗口（请考虑，这个任务管理器进程具有怎样的权限）。

STEP 02 在“进程”选项卡下结束被提升的 explorer.exe 进程，接着关掉任务管理器窗口。

STEP 03 按下“Ctrl+Alt+Del”组合键，打开 Windows 安全界面，然后单击“启动任务管理器”按钮，随后会自动打开任务管理器窗口（这个任务管理器进程的权限又是怎样

的？）。

STEP 04 在“文件”菜单下单击“新建任务（运行）”命令，并在随后出现的“创建新任务”对话框中输入“explorer”，按回车键。

2. 让 UAC 和文件操作和平共处

早在 Windows Vista 的测试阶段曾有测试者戏言，要想在 Windows Vista 的桌面上彻底删除一个文件，包括清空回收站在内，需要 7 个步骤。在早期的测试版中确实存在这个问题，不过随后的正式版已经大幅度简化了这类操作。

然而在 Windows 7 中操作文件的时候，尤其是在操作系统盘的文件时，我们可能还会经常看到 UAC 的“提升”对话框。这主要是因为，为了保证安全性，Windows 操作系统对系统文件设置了比较严格的权限限制，因此，很多文件在使用标准账户或者管理员账户登录后并不能直接修改或者访问（具体的限制则取决于具体的文件用途，以及安全性要求），而是需要在提升后才可以进行。

如果只是偶尔需要对这类文件进行操作，那么提升一下也未尝不可。但如果需要在短时间内操作多个系统文件，那么每个文件操作时都需要提升肯定很烦琐。这时候我们可以使用上文介绍的方法临时绕过 UAC，不过这样并不好，毕竟通过上文的方法，我们可以让执行的所有程序都暂时绕过 UAC，这里我们只是需要对文件进行操作而已。因此，我们只需要以管理员身份启动 Windows 资源管理器程序就可以了，方法如下：

STEP 01 打开“计算机”窗口，按下“Alt”键以显示菜单栏。

STEP 02 依次单击“工具”→“文件夹选项”→“查看”，打开“文件夹选项”对话框的“查看”选项卡。

STEP 03 选中“在单独的进程中打开文件夹窗口”选项，然后单击“确定”按钮。

STEP 04 随后关闭所有已经打开的 Windows 资源管理器窗口。

STEP 05 打开“开始”菜单，在搜索框中输入“资源管理器”，在显示的搜索结果中用鼠标右键单击“Windows 资源管理器”的快捷方式，选择“以管理员身份运行”，并接受 UAC 的提升提示。

STEP 06 随后打开的 Windows 资源管理器窗口就已经具有管理员权限，在该窗口中，我们可以对绝大部分系统文件进行操作，而不用担心权限问题。不过依然有些文件无法操作，因为即使是管理员账户，也没有足够的权限，那些文件只能由系统账户访问，不过在给自己分配相应的权限后，即可访问它（有关权限的分配，请参考本书 5.2 节“NTFS 权限设置”）。

2.2.2.4 解决应用程序兼容问题

除了烦琐的操作，很多人对 UAC 的不满还表现在应用程序的兼容性方面，因为原本可以在 Windows 7 下运行的老程序，因为 UAC 的存在，使用时可能会遇到各种问题。

目前全面兼容 Windows 7 的新版应用程序遇到这类问题很少，因此，我们主要应该关

心一下老版本的程序，如果某个程序在老版本 Windows 中可以正常运行，但在 Windows 7 下无法运行，或者可以运行，但是容易出现一些奇怪的故障，那么可以考虑 UAC 的影响。

例如，某个程序可以在 Windows 7 下正常运行，但每次运行程序并修改了程序的设置后，设置都无法保存，下次启动该程序依然会使用修改前的设置，这可能就是 UAC 在碍事；如果一个程序可以在 Windows 7 下正常运行，但是某些功能无法使用，也有可能是 UAC 的影响。如何在启用 UAC 保证系统安全的前提下让这类程序正常工作？这是本节要讨论的内容。

> **注意**　虽然兼容 Windows 7 的应用程序可能不会因为 UAC 的存在而无法运行，但这并不意味着兼容 Windows 7 的程序在运行的时候不需要提升，这主要取决于程序的类型，以及程序想要进行的操作。例如，一个兼容 Windows 7 的多媒体播放软件，不需要提升就可以正常播放影音文件，但另一个兼容 Windows 7 的磁盘碎片整理软件，因为是工作在系统的底层，需要对文件系统进行操作，尽管它兼容 Windows 7，但依然需要提升后才可以正常工作。这属于正常的设计特性。

那么这里就存在另外一个问题，有些程序在运行的时候会要求提升，只要提升后就可以正常工作在 Windows 7 下。但有些程序（主要是老程序）在运行的时候并没有主动要求提升，并且也无法正常使用（例如，无法保存设置信息），只有提升后才会正常。为什么有些程序可以自动要求提升，有些则不行？其实这是应用程序清单文件在起作用。

默认情况下，兼容 Windows 7 的应用程序使用了一个包含运行级别信息的应用程序清单文件（Application Manifest），该文件帮助操作系统了解该程序所需的特权。应用程序清单文件通过下列方式定义应用程序需要的特权：

- **RunAsInvoker**　使用和当前用户同样的特权运行应用程序，这样，任何用户都可以运行该程序。对于标准用户或者隶属于管理员组的用户，该程序会使用标准访问令牌运行，只有在启动该程序的父进程具有管理员访问令牌的时候，程序才会使用更高的特权运行。例如，如果我们运行了一个提升后的命令提示符窗口，然后从该窗口下启动了一个程序，该程序才会以管理员访问令牌运行。
- **RunAsHighest**　使用当前用户具有的最高特权运行应用程序，这样的程序可以被管理员用户和标准用户运行。可以被程序执行的任务取决于用户的特权，对于标准用户，程序会使用标准访问令牌运行；对于隶属于拥有更高权限的用户组，例如 Backup Operators 组、Server Operators 组或者 Account Operators 组的用户，程序会使用只包含用户当前具有的特权的访问令牌运行；对于隶属于管理员组的用户，程序会使用完整的管理员令牌运行。
- **RunAsAdmin**　使用管理员特权运行应用程序，只有管理员才能运行该程序。对于标准用户或者隶属于拥有更高权限用户组的用户，只有在用户可以通过提升获取更高的权限以进行提升，或者程序通过提升后的父进程启动的情况下（例如，通过提

升后的命令提示符窗口运行该程序），该程序才可以运行；对于隶属于管理员组的用户，该程序会使用管理员访问令牌运行。

清单文件是一个纯文本文件，可以使用任何文本编辑软件（例如，Windows 自带的记事本程序）打开。打开某个软件的清单文件（假设软件的名称是 app.exe，那么对应的清单文件就是 app.exe. manifest）后，可以看到下面的内容：

```
<!-- Identify the application security requirements. -->
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
<security>
<requestedPrivileges>
<requestedExecutionLevel
        level="requireAdministrator"/>
</requestedPrivileges>
</security>
```

其中，“<!-- Identify the application security requirements. -->”这一行注释表示下面开始声明该程序所需的权限，而其中的“level="requireAdministrator"”一行则明确表示如果要运行该程序，必须使用提升后的管理员权限。

因此，当我们在 Windows 7 下试图执行一个程序的时候，系统首先会查找该程序有没有可用的清单文件，如果有，则按照清单文件中的声明来执行，例如，如果清单声明了需要管理员权限，那么系统就会显示 UAC 提升提示对话框供我们操作；如果不存在清单文件，或者清单文件中声明的权限属于标准用户的权限，那么不需要提升，就可以自动开始执行该程序。

这样就很明了了，那些因为 UAC 而无法在 Windows 7 下正常运行的程序，主要就是因为没有提供用于声明所需权限的清单文件。那么这种问题该怎么解决呢？手工编写清单文件吗？不用那么麻烦，因为在 Windows 7 下可以用两种方法让程序以管理员方式运行。

1. 以管理员身份运行程序一次

有时可能偶尔需要用管理员身份运行程序一次，而平时根本不需要使用该程序，或者使用标准用户身份运行即可。对于这类程序，可直接用鼠标右键单击程序的可执行文件或快捷方式的图标，并从右键菜单中选择“以管理员身份运行”命令，如图 2-7 所示。

2. 配置兼容模式总是使用管理员身份运行

如果某个程序是需要经常运行的，那么每次都按照上文介绍的方法进行操作未免有些烦琐，这时候可以通过配置兼容性模式让程序每次都使用管理员身份运行。

在程序对应的可执行文件或者快捷方式的图标上单击鼠标右键，选择“属性”，打开“属性”对话框，接着选择“兼容性”选项卡，随后可以看到如图 2-8 所示的界面。

在“兼容性”选项卡中选中“特权等级”选项下的“以管理员身份运行此程序”选项，这样以后每次直接双击该程序的可执行文件或者快捷方式时，UAC 都会显示提升提示供我们操作。注意，上面的方法只能对当前登录的用户有效，如果这个程序本机的其他用户也需要使用，为了避免每个人都自己设置兼容模式的麻烦操作，可以首先单击“更改所有用户的设置”按钮，在提升之后再选中“以管理员身份运行此程序”选项，这样其他用户在以后不用自己设置也可以使用。

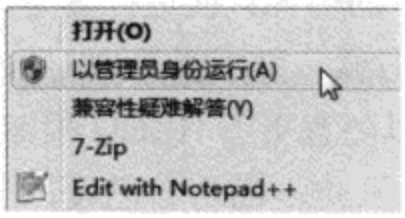


图 2-7　使用管理员身份运行程序

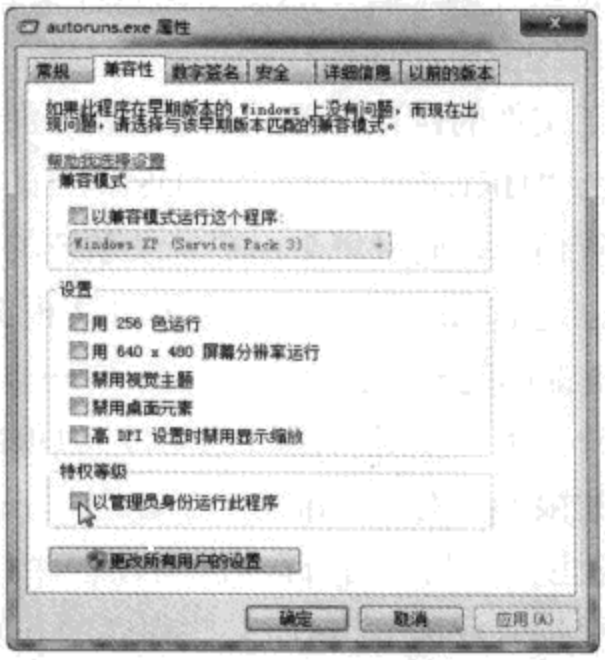


图 2-8　通过兼容性模式让程序总是以管理员身份运行

2.3　文件和注册表虚拟化

对于比较关心技术的读者来说，肯定已经听说过“虚拟化”这个词，并且很多人可能都使用过微软的 Virtual PC 或者 VMware 公司的虚拟机软件，在计算机上虚拟出一台新的计算机出来。不过这里所说的虚拟化可不是虚拟机软件的那个虚拟化。

2.3.1　什么是虚拟化

首先，我们来考虑一个问题，如果某个程序在运行过程中需要将自己的配置信息保存到 Windows 目录下，这种行为到底好不好？毫无疑问，这样并不好，原因有三个：

- 随意给系统文件夹中写入新文件或者修改系统文件，可能会影响到系统的安全性或者稳定性。
- 随意给系统文件夹中写入程序自己的文件，容易让系统文件夹下的文件显得混乱，不易于管理。
- 现在的操作系统已经是多用户的了，而在多用户系统中，如果希望应用程序也能实现多用户的特性(同一台计算机上不同的用户对同一个程序配置可以保持相对独立，其中一个用户的设置不会影响到另一个)，那么程序的配置信息应该保存在每个用户

自己的配置文件夹中，而不是将所有的信息都保存在 Windows 目录下。

然而事实是，虽然多用户操作系统已经发展了多年，而且大部分人都已经在使用多用户操作系统，可是一些第三方软件开发人员依然存在一些不好的习惯，例如软件的默认安装位置是 C 盘根目录（哪怕当前系统根本没有安装在 C 盘），并且安装程序根本不允许选择其他的安装位置；或者软件会把配置信息以.ini 或者作用类似的配置文件的形式保存在 Windows 目录下（注册表是做什么用的？或者如果真的要让自己的软件更“绿色”，为什么不直接将软件的配置信息保存到软件安装目录下？）；甚至一些软件的卸载程序根本不能将程序从系统中干净地卸载掉。

除了文件的保存位置，在注册表方面也存在类似的问题。例如，Windows 的注册表中有一个名为“HKEY_CURRENT_USER”的根键，这个键的主要作用是保存一些和当前用户相关的配置信息，同时每个用户登录系统的时候，Windows 都会根据该用户的配置文件，自动为用户创建 HKEY_CURRENT_USER 根键（也就是说，每个用户自己的 HKEY_CURRENT_USER 根键都是相对独立，并且互不干扰的）。按照设计，每个用户（无论是管理员账户还是标准账户）都可以对自己的 HKEY_CURRENT_USER 根键下的内容直接进行读写，不会受到权限的限制（对于标准用户，在运行 regedit 打开注册表的时候，并不会看到 UAC 提升对话框，这也正是此原因所在，因为在这种情况下，标准用户可以随意更改 HKCU 根键的内容，并不需要提升权限）。然而有些程序的开发人员没有意识到这一点，而将自己设计的程序的配置信息保存在 HKEY_LOCAL_MACHINE，或者其他并非所有的账户都有权限读写的注册表键下，这就导致很多程序只有管理员账户才可以安装和运行，而标准账户甚至连运行都受到了限制。

为了解决文件和注册表中存在的这种问题，微软在 Windows 7 中使用了文件虚拟化和注册表虚拟化技术。简单来说，这种技术类似于一种“重定向”操作，例如，如果某个程序需要在 Windows 目录下写入文件，那么 Windows 会自动将写入操作重定向到另外一个专用的文件夹。但是对于这个程序来说，它确实将文件写入到了 Windows 目录下，同时在该程序试图读取 Windows 目录下的这个文件的时候，Windows 也会将读操作重定向到同一个文件夹中。这样对于这个程序来说，它可以在 Windows 目录下读写文件，但实际上读写的文件并不在 Windows 目录中。

文件虚拟化和注册表虚拟化的工作原理和生效方式类似，但因为对文件的操作比较直观，因此，下文主要以文件虚拟化为例进行介绍。

2.3.2 为什么要使用虚拟化

如何确定虚拟化技术在生效？让我们试试看进行这样的操作：

STEP 01 运行一个兼容 Windows 7 的程序，例如，Windows 7 自带的记事本程序，在记事本中输入一些文字，然后保存该文件。

STEP 02 在选择保存位置的时候，选择当前系统的 Windows 目录，然后保存。

STEP 03 程序会立即做出报告：无法给 Windows 目录下写入文件，同时询问我们是否将该文件保存到其他位置（“文档”文件夹位于当前用户的配置文件中，而用户对于自己的配置文件夹自然是具有所有的权限的），如图 2-9 所示。

在上述这种情况下，虚拟化技术并没有生效，这主要是因为新版本的兼容 Windows 7 的程序可以有效地处理 Windows 在文件夹或者注册表权限方面的限制，那么老的不兼容 Windows 7 的程序会怎么样？

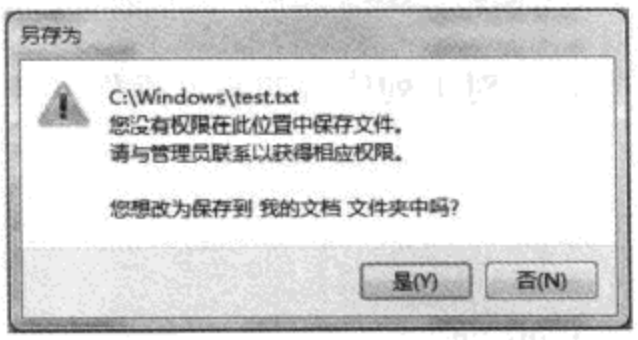


图 2-9　写入操作被限制后会建议将文件写入到其他推荐的位置

让我们再试试看使用一个老版本的程序进行同样的操作，例如，将 Windows XP 中的 notepad.exe 文件复制到 Windows 7 系统中运行，然后尝试将一个文件保存到 Windows 目录下。此时没有任何提示信息，成功地保存好了。难道老程序可以绕过 Windows 目录的权限设置？

让我们用 Windows 资源管理器打开 Windows 目录，这里面并没有出现我们之前保存的 Test.txt 文件，那么这个文件到底被保存到哪里了？注意看资源管理器窗口的工具栏，上面多出了一个“兼容性文件”按钮，如图 2-10 所示。单击这个按钮后，资源管理器窗口会自动进入到另外一个文件夹，如图 2-11 所示。请留意地址栏显示的地址，以及文件夹中的内容。原来我们打算保存到 Windows 目录下的文件被重定向到这里了，同时这里可能还有很多其他文件和文件夹，这些都是被重定向的结果。

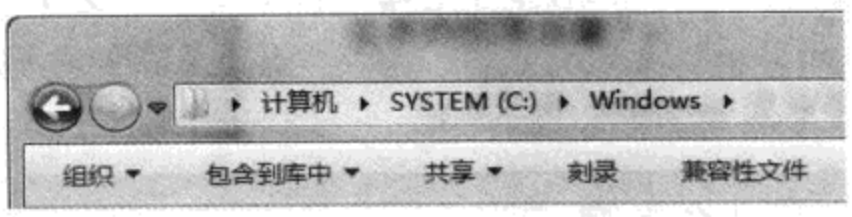


图 2-10　“兼容性文件”按钮的存在意味着写入到这里的文件会被重定向

在重定向到的位置中，请留意地址栏的“VirtualStore（虚拟存储）”文件夹，该文件夹就是用于保存重定向内容的根文件夹。对于每个曾经被重定向过的位置，在该文件夹下都会有对应的子文件夹。例如，按照上文操作后，写入到 Windows 目录的文件被重定向，因此，VirtualStore 文件夹下会创建一个名为“Windows”的子文件夹，所有从系统 Windows 目录重定向的内容都会被写入到这里。

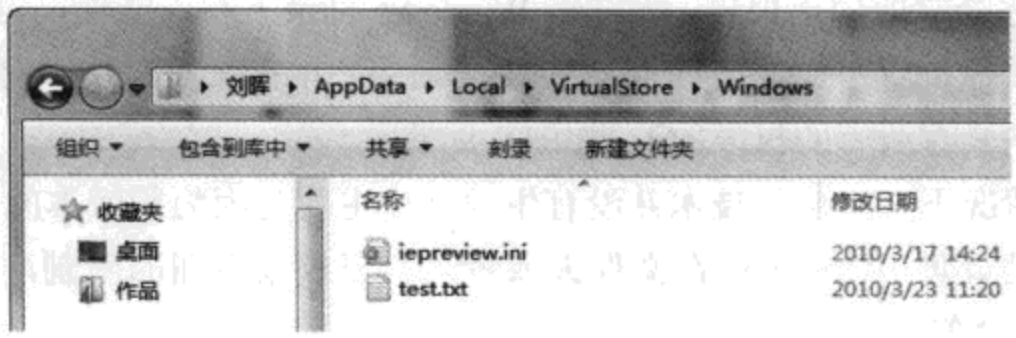


图 2-11　被虚拟化技术重定向的文件都保存在这里

UAC 的虚拟化重定向功能可针对下列位置的写入操作生效：

- %Program Files%。
- %WinDir%。
- %WinDir%\System32。
- HKEY_LOCAL_MACHINE\Software。

用文本文件介绍只是一个例子，假设某个程序需要将配置信息保存到 Windows 目录下，且该程序不兼容 Windows 7，因为无法直接保存，如果没有虚拟化技术，程序可能会报错。但因为有了虚拟化技术，要保存的文件会被自动重定向，这样程序以为自己已经将配置文件保存到了 Windows 目录下，同时程序也确实可以从 Windows 目录下读取到这个配置文件。因此，原本可能无法在 Windows 7 下正常运行的程序因为虚拟化技术的存在，已经可以正常运行了。

另外，请留意图 2-11 中地址栏显示的文件夹地址，被虚拟化技术重定向的文件夹是位于当前用户的配置文件夹中的，这也就意味着每个用户登录到系统后，都有各自独立的虚拟化重定向文件夹，这样一个用户的配置不会影响另一个用户，这不仅保证了兼容性，也保证了安全。

> **注意**　虚拟化技术只会对使用标准令牌运行的程序产生影响，对使用管理员令牌运行的程序无效。而且该技术并不能绝对保证所有不兼容的老程序可以在 Windows 7 下正常运行。

2.3.3　虚拟化对用户有什么影响

按照设计，虚拟化技术应该是一个默默无闻的幕后英雄，因为该技术可以在用户没有察觉到的情况下改善老程序的兼容性，然而有时候可能会存在一些问题。

例如，文件虚拟化技术主要被应用到一些特殊的系统文件夹及其子文件夹中（例如系统盘根目录下的 Windows 文件夹或者 Program Files 文件夹），然而这就存在一个问题，如果我们给系统盘的 Program Files 目录下安装了一个下载软件，默认情况下，该软件下载的文件都会保存在程序的安装目录下，因为虚拟化技术的存在，有可能导致我们找不到下载好的文件。其实这种问题也很好解决，只要用 Windows 资源管理器打开程序的安装目录，

然后单击工具栏上的“兼容性文件”按钮即可。当然，更好的解决办法是配置这个软件，让软件将下载文件保存到其他位置。

2.4　管理存储的凭据

在 Windows 7 中，可以使用凭据管理器将当前用户用于自动登录到服务器、Web 站点，以及其他程序的凭据都保存起来。这些凭据被保存在一个电子保管库（名为 Windows 保管库）中，这样可方便地访问重要的资源，而不需要每次访问都反复输入自己的凭据。同时，这样做还可以实现更简单的单点登录，只需要使用密码登录到自己的 Windows 账户，即可直接登录各种已经保存了密码的网络资源，用一个 Windows 账户密码管理其他所有资源的密码。

Windows 7 的凭据管理器支持下列三种类型凭据的存储：

- **Windows 凭据**　用于进行标准 Windows 身份验证（NTLM 或 Kerberos）使用的凭据，并可包含资源位置、登录账户名称和密码信息。
- **基于证书的凭据**　一种可包含资源位置，并使用保存在证书管理器中个人存储中的证书进行身份验证的凭据。
- **普通凭据**　基本或定制的身份验证技术所用的凭据，其中可包含资源位置、登录账户名称和密码信息。

下文将介绍有关凭据存储方面的内容。

2.4.1　添加 Windows 或普通凭据

每个用户账户都有独立的 Windows 保管库。Windows 保管库中的项目都保存在用户的配置文件设置中，并且其中包含用于登录到受密码保护的资源所需的信息（例如文件服务器的访问路径）。

要给当前登录用户的 Windows 保管库中添加项目，请执行下列操作：

STEP 01　使用希望管理 Windows 保管库项的用户账户登录。打开“开始”菜单，并单击菜单右上角的当前账户的图片，在随后出现的窗口中，单击左侧的“管理您的凭据”链接，随后可以看到如图 2-12 所示的凭据管理器窗口。

STEP 02　按照要创建的凭据类型，分别单击“添加 Windows 凭据”或“添加普通凭据”链接，随后使用提供的选项配置凭据（如图 2-13 所示）。这里需要设置的字段包括：

- **Internet 地址或网络地址**　需要该 Windows 保管库项登录到的网络或 Internet 资源，这里可以输入服务器的名称，例如 FileServer；或输入 Internet 资源的完全合格的域名，例如，www.microsoft.com；或使用包含通配符的地址，例如*.microsoft.com。
- **用户名**　指服务器需要的用户名，例如 Server\User，或者 user@server.com。

图 2-12　查看当前可用的凭据和选项

- **密码**　指服务器需要的密码。这里最容易被忽略的是，如果在服务器或服务上更改了密码，用户还必须更改自己 Windows 保管库中的密码。如果忘了更改 Windows 保管库中的密码，反复尝试登录或连接到服务器或服务，可能导致账户被禁用。

图 2-13　通过设置必要的登录信息即可创建凭据

STEP 03　单击“确定”按钮保存凭据。

2.4.2　添加基于证书的凭据

用户配置文件中保存的个人证书信息包含了颁发给通过身份验证的用户的证书。在为用户添加了证书后，即可为需要使用证书才能访问的资源创建凭据。

要为当前登录的用户的 Windows 保管库内添加基于证书的项，请执行下列操作：

STEP 01　在图 2-12 所示的界面中，单击“添加基于证书的凭据”链接。在“Internet

地址或网络地址”字段中输入要配置该 Windows 保管库项的网络或 Internet 资源的名称，这里可以输入服务器名称、Internet 资源的完全合格的域名或包含通配符的地址。

STEP 02 单击“选择证书”按钮，在“选择证书”对话框中单击访问资源时使用的个人证书，然后单击“确定”按钮。

STEP 03 再次单击“确定”按钮保存凭据。

2.4.3　编辑 Windows 保管库项

我们可以随时编辑 Windows 保管库项的内容，但是要注意，本地 Windows 保管库项只有在创建了这个项目的计算机上才可以看到。这意味着如果想要修改某项，就必须本地登录到创建该项的计算机上。

要编辑用户的 Windows 保管库项，请执行下列操作：

STEP 01 使用希望管理 Windows 保管库项的用户账户登录。打开“开始”菜单，并单击菜单右上角当前账户的图片，在随后出现的窗口中单击左侧的“管理您的凭据”链接。在凭据管理器页面中可以看到所有的凭据按照类型进行分组。

STEP 02 单击希望编辑的凭据项。

STEP 03 单击“编辑”按钮。

STEP 04 根据需要为用户名和密码或该凭据关联的证书进行修改，然后单击“保存”按钮。

2.4.4　备份和还原 Windows 保管库

要备份用户保存的凭据，可以直接备份用户的 Windows 保管库。备份了 Windows 保管库后，即可通过还原 Windows 保管库的方式恢复凭据，或转移到新计算机上。在大部分情况下，我们可以将 Windows 保管库备份到可移动存储介质中。

要备份用户的 Windows 保管库，请执行下列操作：

STEP 01 使用希望管理 Windows 保管库项的用户账户登录。打开“开始”菜单，并单击菜单右上角的当前账户的图片，在随后出现的窗口中单击左侧的“管理您的凭据”链接。

STEP 02 单击“备份保管库”链接。

STEP 03 在存储的用户名和密码页面中，单击“浏览”按钮。使用“将备份文件保存为”对话框选择保存位置，并指定凭据备份文件的名称。凭据备份文件会保存为.crd 文件扩展名。单击“保存”按钮。

STEP 04 单击“下一步”按钮，按下“Ctrl+Alt+Delete”组合键切换到安全桌面。在看到提示后，输入并确认该凭据备份文件的密码。

STEP 05 单击“下一步”按钮，然后单击“完成”按钮。

要将用户的 Windows 保管库还原到同一计算机或不同的计算机，请执行下列操作：

STEP 01 使用希望管理 Windows 保管库项的用户账户登录，按照上文介绍的方法打开

凭据管理器。

STEP 02 在凭据管理器页面中单击“还原保管库”按钮。

STEP 03 在存储的用户名和密码页面中，单击“浏览”按钮。使用“打开备份文件”对话框选择保存了凭据备份文件的位置和文件名，然后单击“打开”按钮。

STEP 04 单击“下一步”按钮，按下“Ctrl+Alt+Delete”组合键切换到安全桌面。在看到提示后，输入凭据备份文件的密码。

STEP 05 单击“下一步”按钮，然后单击“完成”按钮。

2.4.5 删除 Windows 保管库项

如果不再需要某个 Windows 保管库项，我们可以将其删除。要删除用户的 Windows 保管库项，请执行下列操作：

STEP 01 使用希望管理 Windows 保管库项的用户账户登录，打开凭据管理器。

STEP 02 单击希望删除的凭据项。

STEP 03 单击“从保管库中删除”按钮，在要求确认时单击“是”按钮。

CHAPTER

3

第 3 章　策略安全

对于 Windows 7 专业版、企业版和旗舰版，运行“gpedit.msc”后可以打开组策略编辑器，在这里可以对很多隐藏的系统或程序选项进行设置。然而面对众多的策略，你知道这些策略都有什么用吗？怎样设置才能让系统更加安全？

因为 Windows 中包含很多策略，而本书的主题是有关安全的。因此，本章只打算介绍其中影响安全性的策略。要设置这些策略，可以使用本地安全策略编辑器，直接运行“secpol.msc”，这样即可看到组策略编辑器中所有与本地安全有关的策略（如图 3-1 所示）。

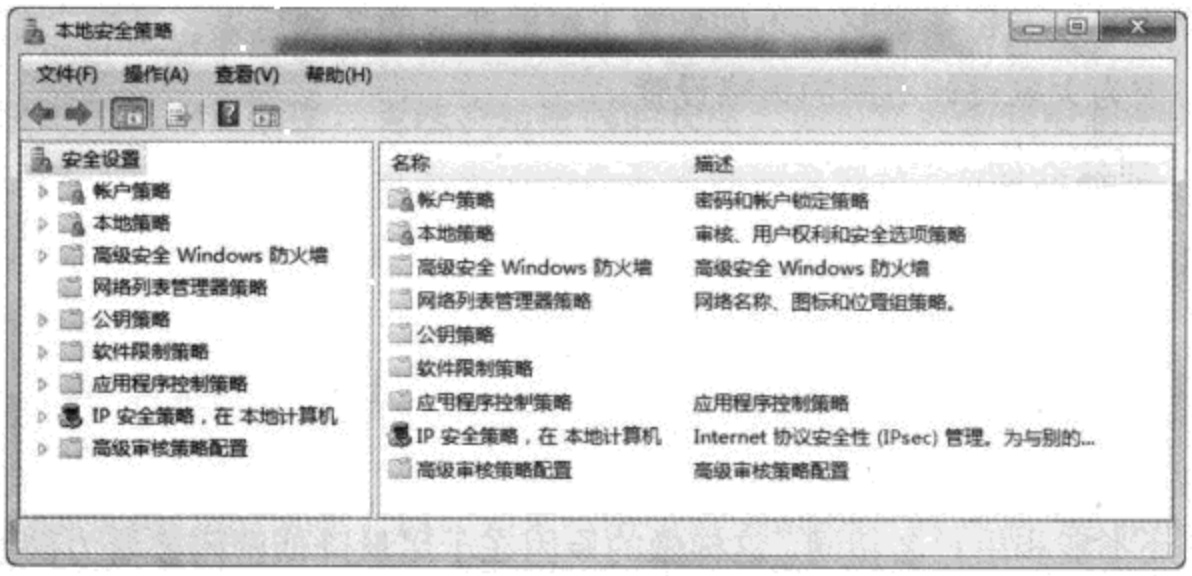


图 3-1　Windows 7 的本地安全策略编辑器

在继续阅读下文之前需要注意一点，下文介绍的很多策略都是用于服务器版 Windows 操作系统和带有 Active Directory 域环境的（虽然这些策略都出现在“本地安全策略”编辑器中），并不适用于单机或者工作组环境下的客户端 Windows 操作系统。然而因为各种原因，这些策略仍然会出现在单机或工作组中的客户端操作系统上。因此，对于这类策略，本书只打算简单介绍其作用，以及相应的安全知识，不具体介绍其使用方法。本章将重点介绍在单机环境下就可以用于加强客户端 Windows 操作系统安全的策略。

另外，Windows 7 家庭版虽然没有组策略功能，但组策略编辑器实际上只是通过一个更加友好的图形界面对注册表进行编辑的工具，完全可以通过直接编辑注册表的方式间接实现组策略编辑器可进行的设置。有关组策略编辑器中的策略和注册表键值的对应关系，

请参考微软发布的参考文档，它的下载地址是：http://tinyurl.com/ybglfvs，该页面提供了针对 Windows Server 2003/2008，以及 Windows Vista/7 操作系统的内容下载。如果没有安装 Microsoft Excel 或者其他任何可以打开.xls 格式文件的软件，还可以在微软网站免费下载 Excel 文件查看器，下载地址是：http://tinyurl.com/yfumezn。

3.1 账户策略

账户策略仅涉及和用户账户的凭据有关的设置，例如，账户密码的复杂性要求、密码的存活时间等。通过设置账户策略，我们能让所有的本地账户更加安全，同时使破解账户密码所需的时间和技术要求会更高。

账户策略分为两大类：密码策略和账户锁定策略。其中，密码策略控制了账户密码的使用情况，而账户锁定策略则决定了在什么情况下锁定账户，锁定多长时间。

3.1.1 密码策略

在密码策略类别中有 6 条策略，本节将首先介绍每条策略的作用、涉及的安全原理、默认值和推荐值，以及每条策略在不同配置下可能造成的各种后果。最后，我们还会根据不同的安全要求为大家设计不同的策略设置。

3.1.1.1 策略介绍

1. 密码必须符合复杂性要求

在 Windows 中，密码策略的默认设置是“已禁用”。

该策略可以强制加强账户密码的安全级别，但安全的密码必须满足下列要求：密码中至少应该包含大写字母、小写字母、数字和特殊字符（例如标点符号）这四类元素中的三种，同时密码还不能和用户名相同。这样做的原因在于尽量降低密码被暴力破解的可能性，因为有很多破解工具可以利用穷举法测试每一组可能的字符组合，以便能猜测出正确的密码。而根据计算，在密码的长度和复杂性增加的情况下，通过穷举法猜测密码的难度和所需时间将会成指数形式增长。因此，一个好的密码完全可以避免在短时间内被猜测出来。有关安全的密码的详细信息，请参考本书 1.3.1.3 节设置安全的密码。

一个可选的用来加强密码复杂性的方法是使用不在默认字符集中的字符。举例来说，使用 Unicode 字符集中从 0128 到 0159 的字符，这种做法有两个好处：它们使得密码的 LanMan 哈希值不可用，而且常用的密码字典都不包含这些字符。然而使用这类字符作为密码也一定不能大意，要输入这样的 Unicode 字符，可以在按下“Alt”键的同时，在数字小键盘上输入代表该字符的数字，输入完四位数字后松开按下的“Alt”键，对应的 Unicode 字符就会被输入进去。

窍门　LanMan 哈希是什么意思？

LanMan 哈希的全称是 Lan Manager Hash，有时被简称为 LM Hash，这是一种密码验证体系。在第 2 章我们已经了解到，在单机或工作组环境下，本地账户的密码在保存到 SAM 数据库后会被加密，而 LM 哈希就是其中一种加密方式。LM 哈希的安全性不是很高，因此，后来还出现了 NTLM2 和 Kerberos 这两种验证体系。对于 Windows NT 4 以及早期版本的 Windows，只支持 LM 哈希，不过对新的 Windows 操作系统，使用后面两种验证体系明显更加安全、可靠，同时可以增加密码被暴力破解的难度。

该策略会在用户下次更改密码的时候生效，已有的密码是不受这个策略影响的。同时，在启用该策略后，如果用户试图使用一个不符合要求的密码，Windows 将拒绝，直到用户提供一个符合要求的密码为止。

2. 密码长度最小值

在 Windows 中，该策略的默认设置是“0”个字符，同时可以设置为 1～14 之间的一个整数。

上文已经说过，为了增加破解密码的难度，应该尽量使用长的复杂的密码。然而上一条策略只能决定密码的复杂度，无法决定密码的长度。如果需要强制限制密码的长度，则可以启用该策略。注意，该策略只对密码的最小长度提出要求，例如，如果设置最小值为“14 个字符”，那么 13 个字符的密码不会被接受，只有长度为 14 个或者超过 14 个字符的密码才会被接受。

实际上，Windows 2000 之后的 Windows 操作系统最多支持长达 127 个字符的密码。长度超过 14 个字符的密码有一个很明显的优势，这种密码没有 LM 哈希，也就只能使用 NTLM2 或者 Kerberos 进行加密。然而如果网络中有 Windows 9x 或者 Windows NT 4.0，以及更早期的计算机，这类系统提供的密码输入框根本无法输入长度超过 14 个字符的密码，因此需要注意，以免引起兼容性问题。

3. 密码最短使用期限

在 Windows 中，该策略的默认值是 0（天），同时可以设置为 1~998 之间的一个整数。

一种比较安全的做法是每隔一段时间更换一次密码，这样，别人就算已经获取了本机的 SAM 数据库，使用破解软件破解密码，可能因为密码过于复杂，等算出密码后，用户已经更换了新的密码使用。这样，可以在老密码被破解后依然保证系统安全。

该策略决定了用户在设置了一个密码后最少要经过多长时间（以天为单位）才能更换新的密码，默认的设置“0”可以让用户随时更换密码，哪怕原先的密码是刚设置的。该策略可以有效地预防用户怕麻烦将原本复杂的老密码修改为一个不那么复杂的新密码后立刻更改回原来复杂的老密码，以实现一直使用同一个复杂密码的不安全做法。

4. 密码最长使用期限

在 Windows 中，该策略的默认值是 42（天），同时可以设置为 0~998 之间的一个整数。

和上一个策略相反，该策略决定了密码可以使用的最长时间（以天为单位），也就是说，一个密码在使用多长时间后就必须更换。

通常情况下，建议将该策略设置为 30，这样在密码快要到期的时候，用户每次登录系统后都会看到系统提示，要求修改密码。在用户修改了密码后，该策略会重新开始统计，并在新密码快到期的时候再次进行提示。

5. 强制密码历史

在 Windows 中，该策略的默认值是“0 个记住的密码”，同时可以设置为 0~24 之间的一个整数。

该策略主要是为了防止用户将几个密码轮换使用。例如，很多人会因为觉得密码复杂性策略设置得太复杂而懒得想新的安全密码，就轮换使用几个密码。而配置该策略后，用户如果愿意轮换使用多个密码，至少必须准备该策略设置的数值个复杂密码来轮换使用。假设将该策略设置为“5”，那么系统就允许用户最多轮换使用 5 个不同的密码（当然，前提是这些密码都要符合上文介绍的复杂性和长度要求）。

这样做也是为了增加密码被破解的难度。请设想这样的情况：有个用户轮换使用两个密码，其中一个是“111i1”，另一个是“22222”，同时策略限制每个密码最多只能使用 30 天。假设有人获取了本机的 SAM 数据库，并通过软件破解出了“11111”这个密码，尽管这时用户可能已经在使用“22222”这个密码了，可 30 天后，该用户依然会换回“11111”这个密码，攻击者就可以在破解出密码后等待一段时间，然后使用这个密码登录到系统（这个假设看似有些极端，但在需要高度安全性的环境中，一定要小心）。

该策略有效地防范了这种攻击，因为系统限制用户如果要循环使用多个密码，必须在指定数量的多个复杂密码之间循环使用。尽管轮换使用几个密码并不安全，但相信 24 个复杂密码轮换使用的安全性至少要比 2 个复杂密码轮换使用要高。

6. 用可还原的加密来存储密码

在 Windows 中，该策略默认是被禁用的，而且一般情况下不建议启用。

该策略决定了是否用双向哈希（Two way Hash）存储加密后的密码，而这样保存的密码就跟明文保存一样，是可以通过哈希反推回密码的。因此，一般情况下，一定要禁用该策略，除非系统中运行的某些应用程序必须要能够知道用户的密码。

3.1.1.2 建议的设置

对于上文介绍的 6 条密码策略，如果网络中都是 Windows 2000 或更高版本的操作系统，建议进行下列设置：

- 密码必须符合复杂性要求：启用。

- 密码长度最小值：14。
- 密码最短使用期限：5 天。
- 密码最长使用期限：30 天。
- 强制密码历史：10 个。
- 用可还原的加密来存储密码：禁用。

如果网络中还包含运行 Windows NT 4 的系统，那么可以将密码长度最小值这一策略设置为“0”，其余设置保持不变。

3.1.2　账户锁定策略

如果攻击者能够在物理上或者远程访问到我们计算机的登录界面，他就可以使用一个用户名和密码进行尝试破解。虽然攻击者基本不可能一两次尝试就能成功登录，但如果不对失败的登录尝试采取一定的限制，时间一长，攻击者就会猜测到正确的密码，并成功登录。

因此，为了实现进一步的安全，必须对失败的登录尝试次数进行一定的限制。这就像银行的 ATM 机，如果连续多次输入错误密码，那么银行卡就会被吃掉，禁止继续尝试输入。而账户锁定策略就可以在满足一定条件的情况下将账户锁定。账户被锁定后，在被管理员解除锁定前，该账户都将无法使用，哪怕可以提供正确的密码。

3.1.2.1　策略介绍

1. 重置账户锁定计数器

在设置“账户锁定阈值”策略前，本策略不会生效。

该策略决定了当一个账户被锁定后，需要等待多长时间（以分钟为单位），系统才自动将记录的失败次数清零。可设置的值是 0～99999，同时该值不能大于锁定时间。

该策略的含义是：假设设置账户锁定阈值为 10 次、账户锁定时间为 60 分钟、复位账户锁定计数器为 30 分钟。如果一位用户忘记了自己的密码，尝试了 5 次就没有继续尝试了，这时候他的账户还没有被锁定，但系统已经记录了失败尝试的次数是 5 次，在最后一次尝试的 30 分钟后，这记录下来的 5 次失败尝试会被清零，等于该用户又有了 10 次尝试机会。

2. 账户锁定时间

在设置“账户锁定阈值”策略前，本策略不会生效。

该策略决定了一个账户在被锁定多长时间（以分钟为单位）后自动被重新启用。可设置的值是 0～99999 之间的整数。

如果将该策略设置为“0”，那么一旦某个账户的失败登录次数达到了“账户锁定阈值”策略的限制，该账户就会被系统自动锁定起来，并且在管理员手工解除锁定之前，该账户将一直处于被锁定的状态。而一旦设置了一个非“0”的值，那么在锁定时间的分钟数达到

该策略的设置后，账户会被系统自动解除锁定。

如果将该策略设置为“0”，就一定要注意，这有可能导致类似“拒绝服务”的攻击。例如，恶意用户可能并不打算非法访问系统，而只是希望制造一点麻烦，让合法用户无法登录。这时候，他只需要故意使用每个账户进行几次失败的登录，以便能够达到账户锁定阈值策略的设置，那么在管理员解除锁定之前，使用该账户的合法用户将无法使用系统。

需要提醒注意的是，系统内建的 Administrator 账户永远不会被锁定。

3. 账户锁定阈值

在 Windows 中，该策略的默认设置是“0 次无效登录”，同时可设置的值是 0～999 之间的一个整数。

该策略决定了允许用户尝试登录的次数，如果失败次数还没有达到设置，用户就可以继续尝试；而一旦达到了次数还没能成功登录，该账户就会被系统自动锁定。

> **提醒** 系统内建的 Administrator 账户不受该策略的影响。

3.1.2.2 建议的设置

对于上文介绍的三条策略，建议这样设置：

- 账户锁定阈值：3 次。
- 账户锁定时间：60 分钟。
- 复位账户锁定计数器：30 分钟。

3.2 本地策略

本地策略中包含的全部是和账户无关的安全设置。通过设置本地策略，我们可以让 Windows 实现更严格的安全性，或者实现其他和安全有关的功能。

3.2.1 审核策略

审核策略可以告诉我们在什么时间、哪位用户在系统中进行了什么样的操作。无论操作是成功还是失败，失败的原因等信息全部都会被审核策略记录起来，供我们查看。因此，在配置好其他安全策略后，最好能根据实际需要对审核策略进行设置，同时还要记得定期查看审核日志，这样就可以将危险扼杀在摇篮中。

需要注意，启用审核（尤其是在审核大量事件）的时候，系统整体运行性能可能会有所降低，同时系统可能会需要大量的硬盘空间保存审核日志。因此，请只在有需要的时候才启用审核，并且要记得定期查看和清理审核日志。

为了避免因为日志满了而无法记录新的访问活动，我们可以通过设置让 Windows 在日志满了之后拒绝用户登录，这需要配置一条安全策略，详细信息请参考 3.2.3 节“安全选项”

中的“审核：如果无法记录安全审核则立即关闭系统”一段的相关内容。

3.2.1.1　策略介绍

默认情况下，Windows 系统不会启用任何审核策略。因此，本节介绍的所有审核策略的默认设置都是禁用的。

1．审核策略更改

该策略决定了是否审核与用户权限分配策略、审核策略或信任策略更改等系统活动有关的事件。如果选择“成功”，那么系统会自动记录有关上述事件的成功操作；如果选择“失败”，那么系统会自动记录有关上述事件的失败操作。注意，“成功”和“失败”可以同时选择。

2．审核登录事件

该策略决定了是否审核每一个登录或注销事件。如果选择“成功”，那么系统会自动记录成功的登录事件；如果选择“失败”，那么系统会自动记录失败的登录事件。“成功”和“失败”可以同时选择。

3．审核对象访问

该策略决定了是否审核与对象访问有关的事件，可供进行访问审核的对象包括文件、文件夹、注册表项、打印机等 Windows 系统中几乎所有可访问的“对象”。如果选择“成功”，那么系统会自动记录启用了审核对象上的成功访问事件；如果选择“失败”，那么系统会自动记录启用了审核对象上的失败访问事件。“成功”和“失败”可以同时选择。

4．审核进程跟踪

该策略决定了是否审核和进程的跟踪信息有关的事件，例如程序的启动和退出、句柄的复制，以及对象访问等活动。如果选择“成功”，那么系统会自动记录有关上述事件的成功操作；如果选择“失败”，那么系统会自动记录有关上述事件的失败操作。“成功”和“失败”可以同时选择。

5．审核目录服务访问

该策略决定了是否审核对具有访问控制列表的活动目录对象的访问情况，简单来说，可以理解为该策略决定了是否审核对活动目录中对象的访问。如果选择“成功”，那么系统会自动记录有关上述事件的成功操作；如果选择“失败”，那么系统会自动记录有关上述事件的失败操作。“成功”和“失败”可以同时选择。

6．审核特权使用

该策略决定了是否审核用户对自己每一项特权的使用情况。如果选择“成功”，那么系统会自动记录有关上述事件的成功操作；如果选择“失败”，那么系统会自动记录有关上述

事件的失败操作。“成功”和“失败”可以同时选择。

7. 审核系统事件

该策略决定了是否审核与重新启动或关闭计算机时，或者对系统安全以及全日志有影响的事件。如果选择“成功”，那么系统会自动记录有关上述事件的成功操作；如果选择“失败”，那么系统会自动记录有关上述事件的失败操作。“成功”和“失败”可以同时选择。

8. 审核账户登录事件

该策略决定了是否审核与（域环境中的）用户登录和注销等活动有关的事件。如果选择“成功”，那么系统会自动记录有关上述事件的成功操作；如果选择“失败”，那么系统会自动记录有关上述事件的失败操作。“成功”和“失败”可以同时选择。

9. 审核账户管理

该策略决定了是否审核和用户管理有关的事件，这些事件包括：

- 创建、更改或删除用户账户或组。
- 重命名、禁用或启用用户账户。
- 设置或更改密码。

如果选择“成功”，那么系统会自动记录有关上述事件的成功操作；如果选择“失败”，那么系统会自动记录有关上述事件的失败操作。“成功”和“失败”可以同时选择。

3.2.1.2 启用审核

审核的操作比较复杂，尤其是要理解不同审核策略可以审核的内容，以及不同审核事件的实际含义。因此，本节会以一般的单机和工作组环境下最常见的问题为例，介绍 Windows 的审核功能：对象访问。

在很多公司中，往往都有这样的要求：有一个文件需要共享到网络上供公司的同事访问，但因为安全原因，管理员必须能够知道谁在什么时间访问过这个文件，这时候就可以考虑使用审核策略，更具体一点，这时候应该使用审核对象访问这个策略。当然，作为可访问的对象，该策略还可以记录很多内容的访问情况，例如打印机或者计算机。

假设在 E 盘的根目录下有一个名为“公司文件”的共享文件夹，我们已经根据需要设置好了共享和相应的权限，现在需要知道每天都有谁在访问这个文件夹中的哪个文件。同时还要知道有没有缺少权限的人尝试访问。这时候请按照下列步骤操作：

STEP 01 运行 secpol.msc 打开本地安全策略编辑器，在左侧的树形图列表中定位到“安全设置”→“本地策略”→“审核策略”。

STEP 02 在右侧窗格中双击“审核对象访问”策略，然后选中“成功”和“失败”选项，单击“确定”按钮保存更改。

STEP 03 打开 Windows 资源管理器窗口，找到“公司文件”这个文件夹，用鼠标右键单击它，选择“属性”，打开“属性”对话框。

- android与iphone及ipad开发书籍 ----------持续不断更新中.....
- c、c++、c#语言pdf书籍及vip视频教程 c、c++、c#、vc等-------持续不断更新中.....
- delphi《书籍》及《视频》教程 ----------持续不断更新中.....
- E网情深VIP系列视频教程 黑客破解菜鸟修练班，VB编程学习班，仿站学习培训，免杀培训，个人系统攻防系列教程，服务器搭建学习班，PHOTOSHOP平面设计班，基础制作论坛（论坛网站搭建），网赚系列教程，网站建设教程，网站漏洞基础，远程控制教程，软件破解班，脚本漏洞提权班
- IT9网络学院VIP系列视频教程 免杀培训班，VMware虚拟机，零基础学习C语言，网游外挂开发精品系列语音教程（外挂教程学习必备研修31课全），VB语言教程30课全，Delphi编程到精通，远程控制软件，加密解密班，网络安全与黑客攻防培训，从入门到精通完整系统化学习C++编程，从入门到精通零基础学习汇编，wordpress教程(个人博客系统49课全)，外行人做易语言盗号和钓鱼程序语音教程 网址：WLSAM168.400GB.COM
- Java书籍 ----------持续不断更新中.....
- photoshop、CorelDRAW、AutocAD等图像处理书籍及vip视频教程 -------持续不断更新中.....
- powerbuilder书籍大全
- Visual Basic语言vip视频教程及pdf书籍 ----------持续不断更新中.....
- windows、linux系统开发、系统封装等pdf书籍及VIP视频教程 ----------持续不断更新中.....
- 《3DS Max》pdf书籍
- 《汇编语言》、《反汇编》及《调试》pdf书籍及vip视频教程 ----------持续不断更新中.....
- 《电子书、电子书、还是电子书》pdf专题库 编程开发，家居美食，儿童益智，人物传记，增强记忆，快速阅读
- 信息系统项目管理师、网络工程师、系统分析师等软考类书籍
- 华中红客系列vip视频教程 脚本攻防培训班，源码免杀培训班，Css语言培训班，C语言，Dreamweaver网页设计，html网页设计培训班，PC安全班， php脚本语言培训班，VMWare虚拟机专题，webshell提权培训班，防站教程，零基础免杀培训班，刷钻速成班，脱壳破解班，外挂编写班，网络赚钱培训班，网站入侵培训班
- 外挂、驱动、逆向及封包视频教程 郁金香、独立团、夜猫论坛、天都吧、看流星论坛、一切从零开始等等
- 安全中国系列vip视频教程 易语言软件编程培训班，ASP.net网站开发项目实战培训班
- 我的收藏
- 按键精灵及TC脚本开发软件视频教程 ----------持续不断更新中.....

当前位置：/《电子书、电子书、还是电子书》pdf专题库

文件名 ⇕

PDF电子书专题库，内容详尽，每天不断更新！！

- 办公类软件使用指南
- 医学
- 历史人物传记
- 哲学宗教
- 外语资料（除英语外） （除英语外）
- 官场类小说
- 建筑工程类
- 情感生活类小说
- 政治军事
- 教育学习科普大全
- 文学理论
- 智力开发、增强记忆、快速阅读技巧大全
- 社会生活
- 科学技术
- 程序编程类
- 经济管理
- 网络安全及管理
- 网赚系列
- 美食小吃烹饪煲汤大全
- 课外读物

本网盘内容太多，持续不断更新，发布各类视频教程、pdf书籍，包括破解、加解密、外挂辅助制作，易语言培训教程、编程语言、网页制作等等，教程及书籍仅用于学习,如用于商业或非法用途的后果自负！

网址：WLSAM168.400GB.COM

- VIP培训教程，易语言黑月VIP视频教程，天都网易语言系列培训教程(100集全)，集中营易语言学习视频(80集)
- 棉猴系列vip视频教程 gh0st远控控制源码讲解教程，套接字编程，DLL程序编写，键盘监听驱动程序编写，驱动基础教程，AsyncSelect模型QQ程序教程，C++语言入门基础，NB5.5源码分析教程
- 游戏开发pdf书籍 ----------持续不断更新中.....
- 炒股投资pdf书籍及视频教程 短线高手系列，短线天王系列，操盘论道系列，翻倍黑马，看盘快速入门，庄家手法大曝光等等。 网址：WLSAM168.400GB.COM
- 热门小说集中营 傲世九重天，网游之三国时代，武动乾坤
- 甲壳虫VIP教程全集 asp教程，Delphi培训班，FLASH培训班，Java培训班，linux培训班，PHP培训班，源码免杀班，甲壳虫C++，脚本功防班，免杀班初、中、高级班，破解班，源码免杀班，脱壳班，易语言培训班，无特征码免杀，网站架构培训班，外挂高级班，外挂初级班第1、2部
- 破解、免杀、入侵、脱壳、攻防及漏洞分析系列VIP视频教程（80多部） 天草、黑客动画吧等等--------持续不断更新中....
- 网站建设相关的pdf书籍及各种vip视频教程 ----------持续不断更新中.....
- 网赚、淘宝系列vip视频教程 网赚30天新人魔鬼训练，屠龙网赚团队vip课程，站长大学网赚视频（50课全），图腾团队日赚1000元竞价行销教程，屠龙团队淘宝宝贝卖疯系列，站群网赚系列，淘宝开店视频，红星挂机日赚10元，百万流量系列，漂流瓶圣手全自动挂机引，贴吧邮件定向营销疯狂成交量月入万元
- 英语学习资料百科大全 不断更新。。。
- 饭客论坛系列VIP视频教程 脚本入侵班，黑客之免杀教程，易语言教程，无线网络攻防教程，入侵教程，delphi系列教程，黑客基础入门
- 黑客书籍 有关黑客、安全、加解密技术等等----------持续不断更新中.....
- 黑手安全网VIP系列视频教程 DIV+CSS网页布局，Dreamweaver教程，flsah动画教程，photoshop教程，跟我一起学C++课程，抓鸡
- 黑鹰、黑基、黑防、黑盾vip系列视频教程 破解提高班66课全，SQL注入，ASP注入教程，完完全全学会抓肉鸡，脱壳破解教程50课全，提权班，C语言特训班26讲全，黑客脚本特训班，黑客工具特训班，dedecms仿站教程，VC编写远控30课全，网页美工特训班，木马免杀特训班，驱动开发技术VIP培训班，外挂破解等等。

- [电脑世界的通关密语：电脑编程基础].(杉浦贤).滕永红.扫描版.pdf
- [程序语言的奥妙：算法解读（四色全彩）].(杉浦贤).李克秋.扫描版.pdf
- [差错：软件错误的致命影响].(帕伯斯).邝宇恒等.扫描版.pdf
- [算法之道（第2版）].邹恒明.扫描版.pdf
- [O'Reilly：深入学习MongoDB].(霍多罗夫).巨成等.扫描版.pdf
- [深入浅出WPF].刘铁猛.扫描版.pdf
- [Go语言·云动力（云计算时代的新型编程语言）].樊虹剑.扫描版.pdf
- [精通.NET互操作：P/ Invoke、C++ Interop和COM Interop].黄际洲等.扫描版.pdf
- [编程的奥秘：.NET软件技术学习与实践].金旭亮.扫描版.pdf
- [O'Reilly：学习OpenCV（中文版）].(布拉德斯基等).于仕琪等.扫描版.pdf
- [Go语言编程].许式伟等.扫描版.pdf 网址：WLSAM168.400GB.COM
- [MySQL技术内幕：SQL编程].姜承尧.扫描版.pdf
- [Tomcat权威指南（第2版）].(布里泰恩等).吴豪等.扫描版.pdf
- [Ext江湖].大漠穷秋.扫描版.pdf
- [IT名人堂·Oracle DBA突击：帮你赢得一份DBA职位].张晓明.扫描版.pdf

Total: 77 1 2 3 4 5 6 ›

STEP 04 打开“属性”对话框的“安全”选项卡，单击“高级”按钮，打开“高级安全设置”对话框。

STEP 05 打开“审核”选项卡，单击“继续”按钮，打开“高级安全设置”对话框的编辑模式。

STEP 06 单击“添加”按钮，打开如图 3-2 所示的“选择用户或组”对话框。

STEP 07 在输入要选择的对象名称框中，输入要审核的用户或者组的名称，然后单击右侧的“检查名称”按钮。

STEP 08 如果输入无误，输入的对象就会被补全为“机器名\用户（组）名”的形式，然后单击“确定”按钮。

STEP 09 随后可以看到如图 3-3 所示的“审核项目”对话框。在这里我们需要选中所有需要审核的访问类型，例如读取、写入、删除等。

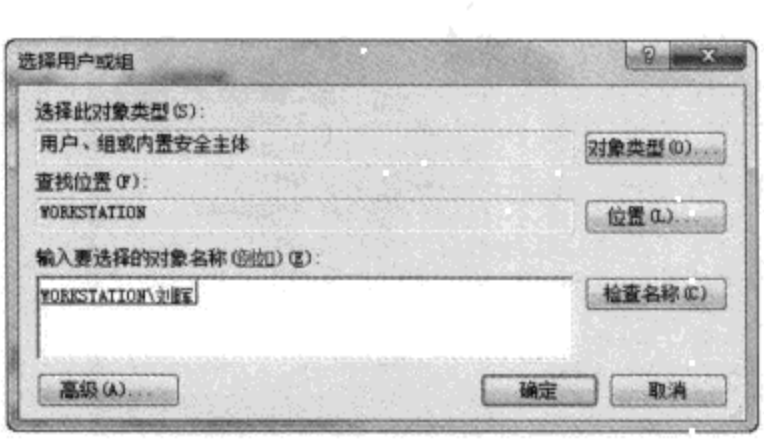


图 3-2　在这里可以添加要审核的用户或组

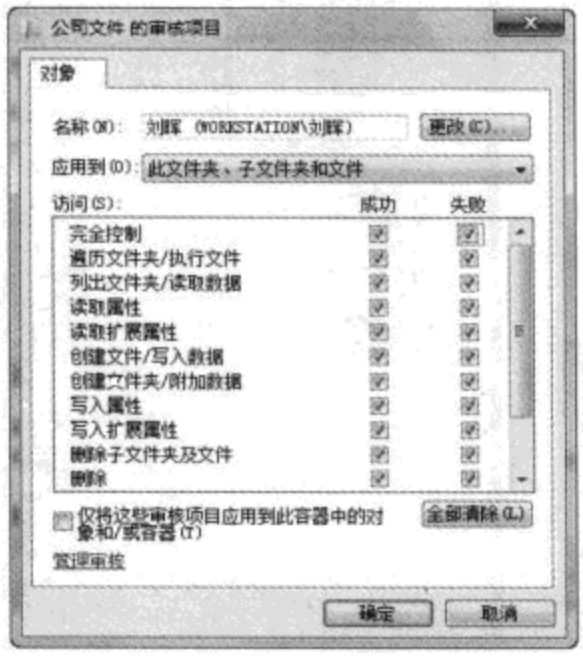


图 3-3　“公司文件的审核项目”对话框

STEP 10 根据实际需要，首先在“应用到”下拉菜单中选择该审核工作的适用范围，例如可以选择应用到该文件夹、子文件夹以及文件，或者只应用到其中的文件等；接着在下方的访问列表中选中所有希望审核的操作类型，同时对于每种类型，我们都可以选择成功或者失败的访问。设置好之后单击“确定”按钮。

STEP 11 如果还需要审核其他用户或者用户组的访问操作，请按照上述步骤添加并进行设置。

STEP 12 全部添加并设置好之后，多次单击“确定”按钮，关闭所有打开的对话框。

接下来就可以像平时那样使用共享文件了。等待一段时间，只要通过事件查看器就可以看到所有与对象访问有关的审核日志内容。

3.2.1.3　查看审核记录

经过一段时间的使用，管理员应该及时查看审核日志，这时需要用到 Windows 事件查

看器。

通过事件查看器查看审核日志的方法如下：

STEP 01 打开“开始”菜单，在“计算机”上单击鼠标右键，选择“管理”，打开计算机管理控制台。

STEP 02 在窗口左侧的控制台树中依次单击进入“计算机管理”→“系统工具”→“事件查看器”→“Windows 日志”→“安全”，接着可以看到如图 3-4 所示的事件查看器主窗口。

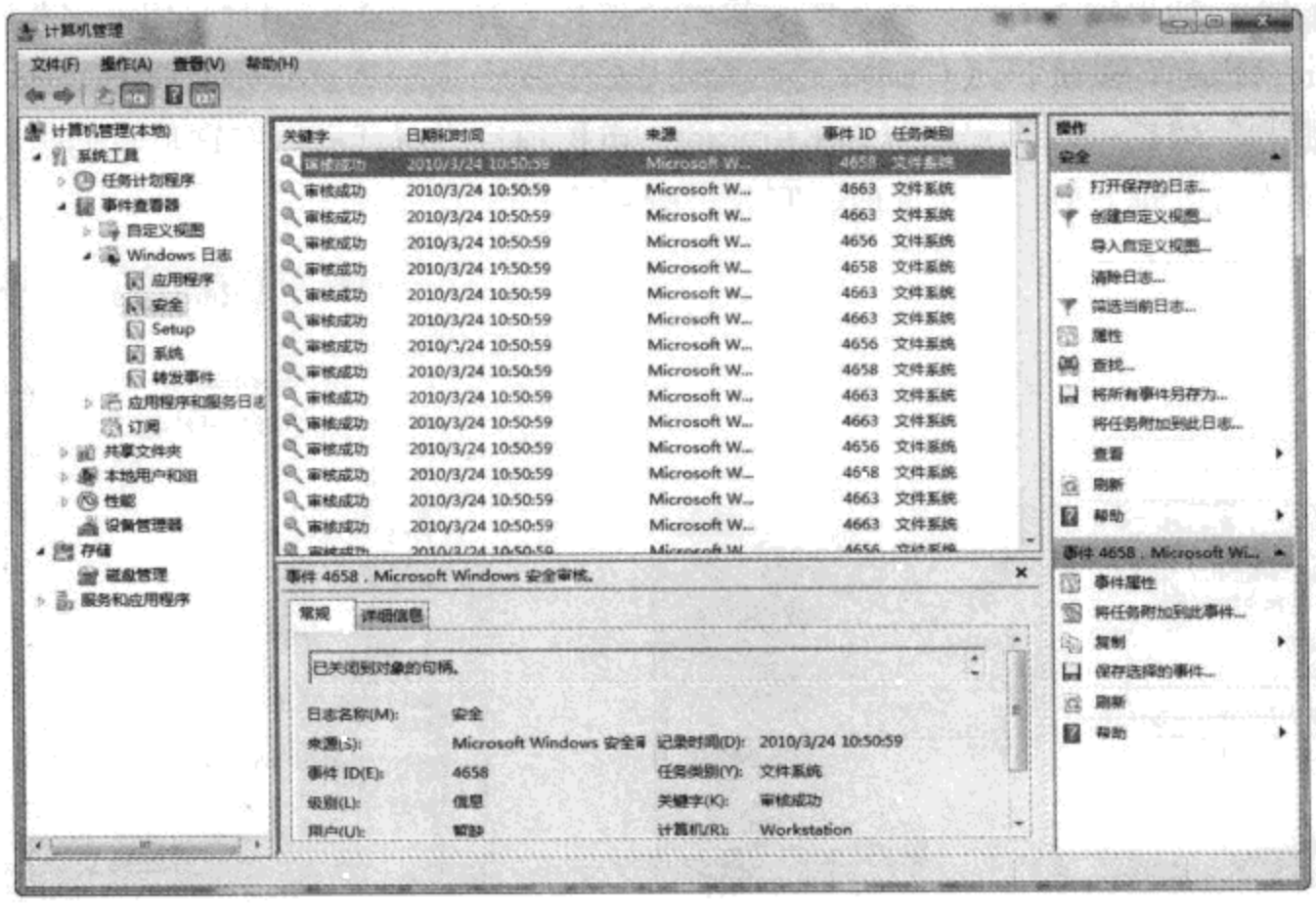


图 3-4　利用事件查看器查看安全审核日志

STEP 03 默认情况下，这里会显示大量和安全有关的日志记录，而安全审核日志只是其中的一部分。因此，为了便于查看，可以利用筛选功能对所有的日志记录进行筛选。在计算机管理窗口右侧的操作窗格中单击“筛选当前日志”按钮，随后可以看到如图 3-5 所示的“筛选当前日志”对话框。

STEP 04 在图 3-5 所示的对话框中根据实际情况选择要看到的事件的选项。例如，如果希望看到和上一节设置的文件访问审核有关的记录，可以分别进行下列设置：

- **记录时间**　这个选项决定了想要看到多长时间内的记录，Windows 7 会自动为我们提供比较接近自然语言的选项，例如“过去的 24 小时”、“过去的 7 天”等。当然，如果预设的选项无法满足需要，可以从这个下拉菜单中选择“自定义范围”，然后选择自定义的时间段。
- **事件级别**　这个选项决定了要看到哪些级别的事件。通常来说，在 Windows 7 中有

关键、警告、详细、错误和信息这 5 个不同的级别，而关于文件的安全审核，大部分事件都属于“信息”级别的，另外，可能有少数属于“警告”或者“错误”级别，因此，可以选中这三个级别，或者一个都不选，这样事件查看器将不对事件级别进行筛选（也就是说，显示所有级别的事件）。

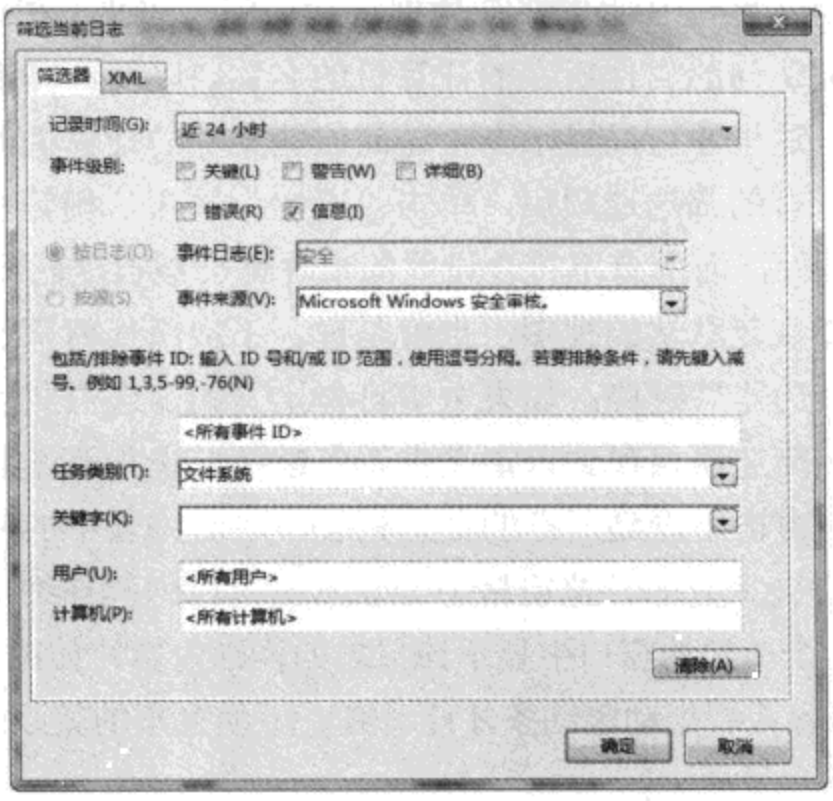


图 3-5　通过筛选功能找出希望看到的审核日志

- **按日志**　因为之前已经从窗口左侧的控制台树中进入了“安全”日志，因此，“按日志”选项是灰色的。如果进入的是“Windows 日志”或者其他节点，那么将可以通过该选项选择要筛选的日志。
- **按源**　事件的来源是多种多样的，而这个下拉菜单会根据所选事件的类型提供所有的来源选项。因为需要查看的是审核策略，因此，可以在事件来源下拉菜单中选择“Microsoft Windows 安全审核”。如果需要，还可以同时选择其他来源。
- **事件 ID**　接着可以在标有“所有事件 ID”的文本框中输入要查看的事件的 ID。如果只希望查看特定 ID 的事件，那么可以直接输入事件 ID，如果需要输入多个 ID，不同 ID 之间可以使用半角逗号（,）隔开。
- **任务类别**　因为要查看的是和对象访问有关的审核日志，更具体地说，要查看的是与文件和文件夹的访问有关的审核日志。因此，可以在这里选择“文件系统”。当然，如果需要，还可以直接在这里选择多种不同的类别，例如注册表。
- **关键字**　在这个下拉菜单中可以选择要查看的事件的关键字，例如，如果希望看到所有访问成功的事件，可以选择“审核成功”；如果要查看所有访问失败的事件，可以选择“审核失败”。
- **用户**　在标有“所有用户”字样的文本框中，可以输入一个用户的名称，只查看和

该用户有关的审核日志。

- **计算机** 在标有“所有计算机”字样的文本框中可以输入一个计算机的名称，只查看通过这台计算机进行访问时的审核日志。这里需要注意，在单机和工作组环境下，因为每台计算机独立维护各自的 SAM 数据库，而我们从计算机 A 上访问计算机 B，实际上是在使用计算机 B 上的账户凭据进行访问。因此，在这种环境下，“计算机”一栏只能显示被访问的文件所在的计算机的名称，以及计算机 B 上的账户名称。只有在域环境下，这里才可以显示真正访问这些文件的计算机的名称。

STEP 05 设置好所有的筛选选项后，单击“确定”按钮，稍等片刻，事件查看器就会显示所有符合设置的事件，而所有不符合设置的事件都会被自动隐藏（而非删除）。

STEP 06 如果需要恢复默认的视图，也就是说，不应用任何筛选，可以单击窗口右侧操作窗格中的“清除筛选器”链接；如果希望将自定义的筛选方式保存起来，以便以后直接使用，可以单击“将筛选器保存到自定义查看”链接。进行筛选后，即可在计算机管理控制台窗口中央上方的窗格中看到所有的日志列表，单击列表中的任何一条日志后，在计算机管理控制台窗口中央下方的预览窗格中会显示出该日志的详细信息。双击任何一条日志，Windows 就会在一个单独的窗口中显示该日志的详细内容，如图 3-6 所示。由于对话框面积有限，大部分的内容需要拖动滚动条才能看到。下面列举的就是这些内容的一个例子：

```
试图访问对象。
对象:
    安全 ID:      Workstation\刘晖
    账户名:       刘晖
    账户域:       Workstation
    登录 ID:      0x48b9e
对象:
    对象服务器:   Security
    对象类型:File
    对象名:  D:\公司文件
    句柄 ID: 0x67c
进程信息:
    进程 ID: 0x1960
    进程名:  C:\Windows\explorer.exe
访问请求信息:
    访问:     ReadAttributes
    访问掩码:0x80
```

在图 3-6 所示的日志中，除了上文介绍过的一些内容的作用，还有一些内容需要注意，这些内容是：

- **安全 ID** 显示了导致这个事件的账户的名称，以及所在计算机。
- **对象类型** 显示了这条日志是在访问什么对象的时候产生的，例如文件、文件夹或者注册表项。
- **对象名** 显示了具体被访问的对象，例如，如果审核的是文件或文件夹，这里会显

示这个文件或文件夹在本地计算机上的路径和名称（也就是说，显示的是“e:\公司文件”，而非“\\Workstation\公司文件\”）。

- **记录时间**　显示了访问该对象的具体时间。
- **关键字**　显示了访问的结果，例如是成功或者是失败。

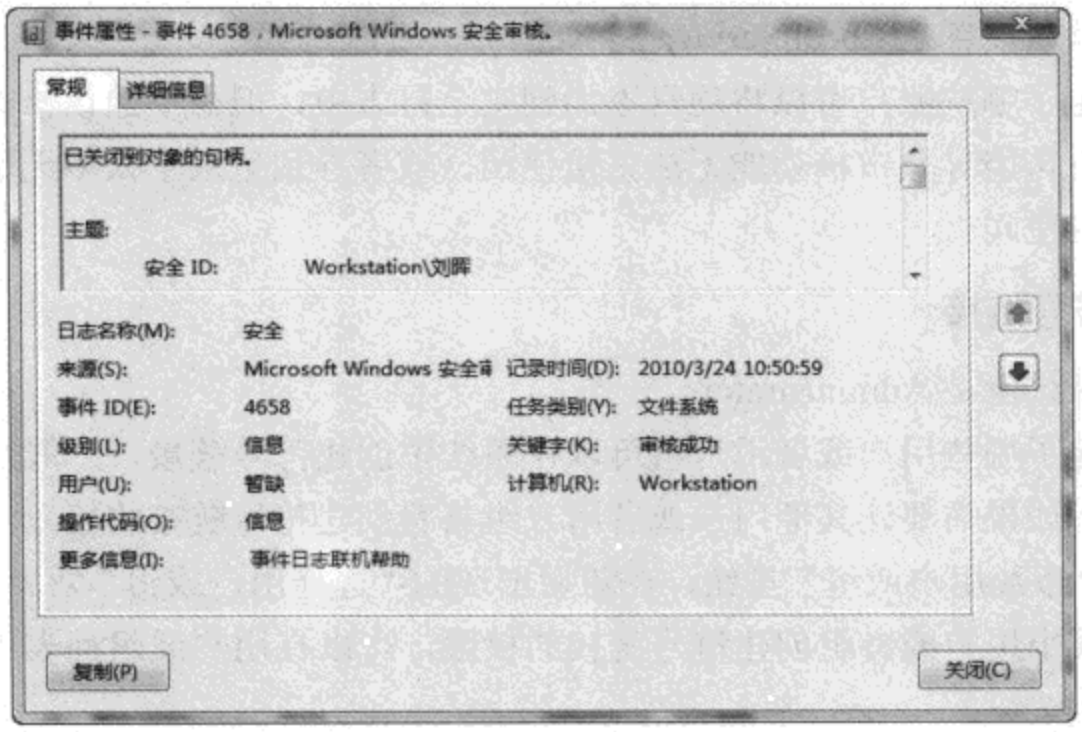


图 3-6　日志文件的详细内容

上文简单介绍了如何在 Windows 中进行审核，以及如何查看审核结果。相信大家已经对审核的大致操作有所了解。现在可以考虑一下，如果希望看到某个用户对注册表的访问情况，应该如何设置审核，同时在查看审核日志的时候应该如何筛选。

3.2.2　用户权限分配

在第 1 章中介绍过用户以及用户组的概念，通过阅读第 1 章，我们应该已经了解，不同的用户或者不同的用户组具有不同的特权。那么如何给自己创建的用户组分配所需的特权呢？这些操作可以通过本地安全策略编辑器中的用户权限分配策略进行设置。

1．备份文件和目录

该策略的默认设置是 Administrators 和 Backup Operators。

在 Windows 中，备份是一种比较特殊的操作，因为一个人如果具有备份文件的权限，那么就算他没有访问某个文件的权限，也一样可以使用备份工具（可以是系统自带的备份工具，也可以是其他兼容备份行业标准的第三方专用备份工具）对该文件创建备份。更详细地说，该组的用户或者用户组将对本机的所有文件和文件夹具有遍历文件夹/执行文件、列出文件夹/读取数据、读取属性、读取扩展属性，以及读取权限的权限。

因此，给其他用户或者用户组指派备份权限的时候一定要十分小心，尽量不要给太多的人这种权限。如果需要让其他用户或者用户组具有备份文件的权限，可以打开该策略，

然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的备份权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

2. 生成安全审核

该策略的默认设置是 Local Service 和 Network Service。

该策略决定了哪些账户可以将项目添加到安全日志中，但是不建议修改默认设置，因为错误的设置有可能导致审核功能无法正常使用，或者导致记录了太多无用的事件，浪费系统资源和硬盘空间。

3. 创建符号链接

该策略的默认值是 Administrators。

该策略决定了哪些用户或者用户组可以在系统中创建符号链接，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有创建符号链接的权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组创建符号链接的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

那么什么是符号链接？它有什么作用？符号链接（Symbolic Link）原本是 UNIX 操作系统中的一项功能，从 Windows 2000 开始出现在 Windows 操作系统中，这个功能可以给系统中不同的对象之间创建链接。在 Windows Vista 之前，Windows 中的符号链接功能只能用于 NTFS 硬盘分区/卷或者文件夹，不能用于单独的文件，而从 Windows Vista 开始，符号链接可用于文件。

列举一个更形象的例子吧。在 Windows 7 中，使用管理员身份启动一个命令提示行窗口，进入到当前用户的“桌面”目录下，然后运行下列命令：

```
Mklink /d Sysroot %systemroot%
```

接着回到桌面上，我们将发现一个类似快捷方式的图标，双击该图标可以打开 Windows 目录。那么用命令创建的符号链接和快捷方式有什么区别？试试看用 Windows 资源管理器打开系统盘，然后用鼠标右键单击 Windows 目录，指向“发送到”，选择“桌面快捷方式”，在桌面上创建一个真正的快捷方式。接着分别用鼠标右键单击快捷方式和符号链接，选择“属性”，打开“属性”对话框，如图 3-7 所示，对比一下有什么不同。

在图 3-7 中的左图是真正的“快捷方式的属性”对话框，右图是“符号链接的属性”对话框。从图中的“常规”选项卡中就可以看出，对于快捷方式，实际上是保存在桌面上的一个“.lnk”文件，因此，快捷方式实际上具有文件的所有属性；而对于符号链接，则表现出了和真正文件夹一样的属性，我们不仅可以通过符号链接就能得知其对应文件夹占用的硬盘空间，同时还可以像直接操作文件夹那样设置访问权限或者使用卷影复制。

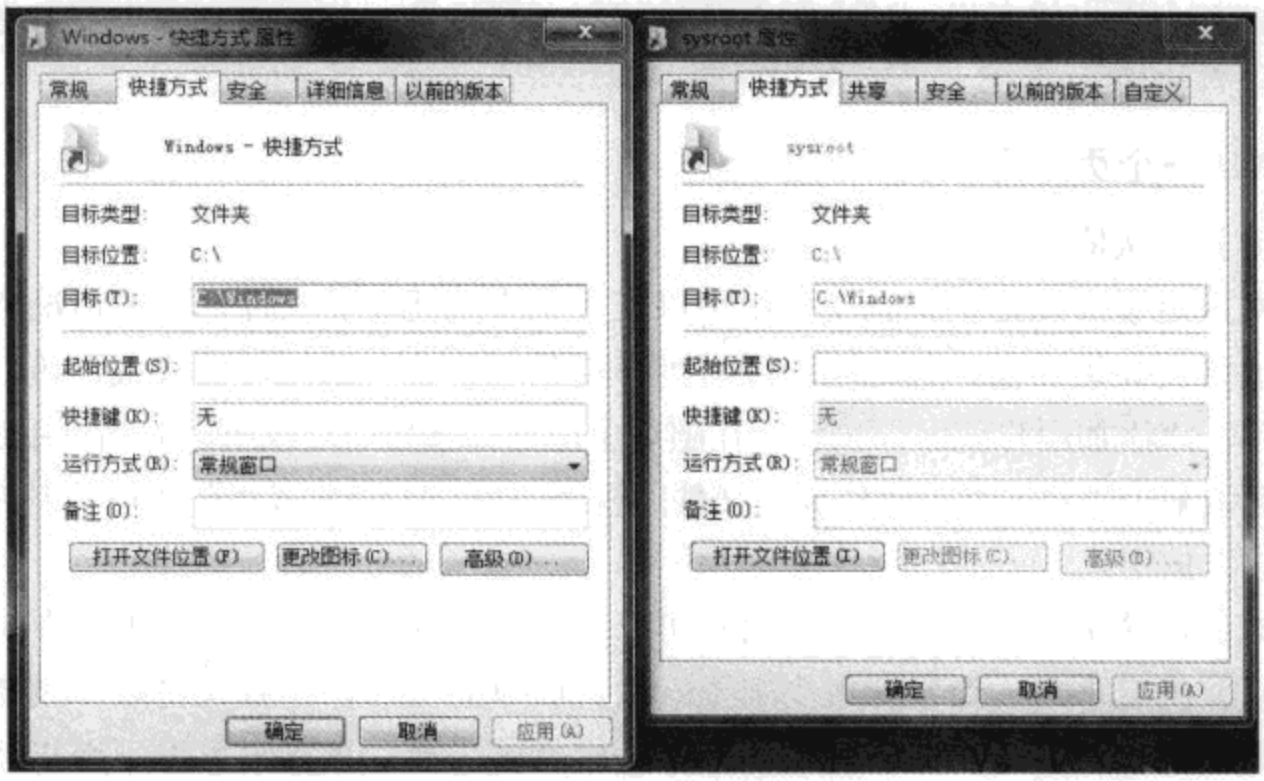


图 3-7　快捷方式的属性和符号链接的属性

当然，“快捷方式（.lnk 文件）的属性”对话框中也有设置访问权限的“安全”选项卡，以及使用卷影复制“以前的版本”选项卡，但这两个选项卡都只能作用于这个.lnk 文件本身，并不能用于其对应的文件夹。

关于符号链接的作用和更详细的使用方法，并不属于本书的讨论范围，因此，不准备过多地介绍。感兴趣的读者请自己查阅相关文档。

4．创建全局对象

该策略的默认值是 Administrators、Local Service、Network Service，以及 Service。

该策略决定了哪些用户或者用户组可以在系统中创建全局对象，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有创建全局对象的权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组创建全局对象的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

那么全局对象又是什么？全局对象是指可以被所有的会话访问的对象，而没有该权限的用户只能创建和自己的会话有关的对象。因为能够创建全局对象的用户可以影响到其他用户的会话，因此，通常情况下不建议给一般用户指派这个权限。

5．创建一个令牌对象

该策略的默认值是空的。

该策略决定了哪些用户或者用户组可以在系统中创建令牌对象，一般情况下不建议更改该设置。如果需要让其他用户或者用户组具有创建令牌对象的权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如

果希望撤销某个用户或者组创建令牌对象的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

6. 创建一个页面文件

该策略的默认值是 Administrators。

该策略决定了哪些用户或者用户组可以在系统中创建页面文件，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有创建页面文件的权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组创建页面文件的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

简单地说，这个策略决定了哪些用户可以修改系统的分页文件（虚拟内存）设置。因为该设置只要确定下来，通常就很少需要修改，所以完全可以由管理员账户设置好后保持固定不变。因此，通常情况下，如果不是因为有特殊需要，该权限可以不用指派给管理员之外的其他任何用户或用户组。

7. 创建永久共享对象

该策略的默认值是空的。

该策略决定了哪些用户或者用户组可以在系统中创建永久共享对象，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有创建永久共享对象的权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组创建永久共享对象的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

永久共享对象包括设备、信号量（Semaphore）以及互斥（Mutexe）等，这个权限对需要扩展对象命名空间的内核模式系统组件非常有用。因此，一般情况下不用修改设置。

8. 从扩展坞上取下计算机

该策略的默认值是 Administrators 和 Users。

该策略决定了哪些用户或者用户组可以将计算机和扩展坞断开。如果需要让其他用户或者用户组具有断开扩展坞的权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组断开扩展坞的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

这条策略主要用于笔记本电脑，扩展坞可以增强笔记本电脑的输入和输出功能。例如，将笔记本电脑连接到扩展坞后，笔记本电脑可能就有了原本不具备的功能，例如，增加额外的电池或者硬盘，增加性能更强劲的显卡，或者增加多声道音频输出功能等。扩展坞可以实现的具体功能取决于具体的产品，注意，并不是每种型号的笔记本电脑都可以连接扩展坞。详细情况请参考笔记本电脑或者扩展坞的说明文件。

需要注意，没有该权限的用户只是无法将扩展坞正常弹出而已，但实际上，用户依然可以强制将扩展坞和笔记本电脑之间的连接断开。就像 USB 设备的拔出，正常以及安全的做法是在拔出这类设备之前首先将其与计算机断开（逻辑上的），然后将设备从 USB 接口上拔出（物理上的）。当然，不从逻辑上断开也可以直接从物理上拔出，但这有可能导致系统崩溃或者数据丢失（尤其是扩展坞中可能还存在和系统运行至关重要的设备，例如第二块硬盘、外接显卡或者智能卡读卡器等）。

9. 从网络访问此计算机

该策略的默认值是 Administrators、Backup Operators、Everyone，以及 Users。

该策略决定了哪些用户或者用户组可以通过网络访问本机。如果需要允许其他用户或者用户组通过网络访问本机，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望拒绝某个曾经允许的用户或者组通过网络访问本机，可以在用户或组列表中将其选中，然后单击“删除”按钮。

注意　这个策略对远程桌面，以及远程协助等终端服务的应用无效。

10. 从远程系统强制关机

该策略的默认值是 Administrators。

该策略决定了哪些用户或者用户组可以从远程系统关闭计算机。如果需要让其他用户或者用户组具有这种权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这种权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

这个功能更多的是应用于服务器领域的，因为服务器通常都需要长时间连续地运行，但有时候又需要接受用户的远程访问。禁止用户从远程系统强制关机，可以避免用户在远程登录的时候无意中关掉了服务器，而又无法立刻打开（毕竟除了网络唤醒，要想打开一台关闭的计算机，绝大部分时候都得亲自到计算机前按下电源按钮）可能带来的麻烦。

11. 更改时区

该策略的默认值是 Administrators、Local Service 以及 Users。

顾名思义，该策略决定了哪些用户或者用户组可以更改系统时区设置，一般情况下没必要修改这里的设置。如果需要让其他用户或者用户组具有更改系统时区设置的权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组更改系统时区设置的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

12. 更改系统时间

该策略的默认值是 Administrators 和 Local Service。

该策略决定了哪些用户或者用户组可以更改系统时间，一般情况下，如果需要通过网络进行 Kerbores 验证，或者有其他应用密切要求整个网络中的所有计算机都具有一致的时间，那么就应该严格控制可以修改系统时间的人的数量。但对于一般的单机和工作组环境，往往没有这种需要。如果需要让其他用户或者用户组具有修改系统时间的权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组修改系统时间的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

13. 关闭系统

该策略的默认值是 Administrators、Backup Operators 以及 Users。

该策略决定了哪些用户或者用户组可以在本地关闭系统。如果需要让其他用户或者用户组具有从本地关闭系统的权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组从本地关闭系统的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

该策略和“从远程系统强制关机”策略类似，最主要的应用还是在服务器上。因为服务器是不能随便关闭的，但一般情况下，对于客户端计算机，很少会有这种需要。

14. 管理审核和安全日志

该策略的默认值是 Administrators。

该策略决定了哪些用户或者用户组可以在系统中管理审核和安全日志。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的该权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

该策略的作用和“产生安全审核/生成安全审核”策略的功能是相辅相成的。前者决定了谁可以查看审核产生的日志内容，后者决定了谁可以设置系统以进行审核。

15. 还原文件和目录

该策略的默认值是 Administrators 和 Backup Operators。

该策略决定了哪些用户或者用户组可以使用系统自带的备份程序还原之前备份的文件，哪怕他并没有访问或者替换这些文件的权限。如果需要让其他用户或者用户组具有还原文件的权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组还原文件的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

它与“备份文件和目录”策略类似，可以让具有还原权限的人对本机上的所有文件和文件夹具有遍历文件夹/执行文件以及写入的权限。因此，给别人指派该权限的时候一定要小心，如果有恶意的人具有了该权限，他虽然不能读取机密文件的内容，但完全可以用备

份文件中过时的机密文件替换该文件的最新版本，导致一定的损失。

16. 加载和卸载设备驱动程序

该策略的默认值是 Administrators。

该策略决定了哪些用户或者用户组可以在系统中安装或者卸载设备驱动。如果需要让其他用户或者用户组具有安装或卸载设备驱动的权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

> **注意**　因为大部分设备的驱动程序都工作在系统底层，甚至依然工作在内核模式下，因此，驱动程序对整个系统的稳定性和安全性有重大的影响。例如，如果某个硬件设备的驱动编写不够完善，那么很可能导致各种怪异的问题，例如设备无法正常工作，或者系统频繁遭遇蓝屏死机等问题。更严重的是，和很多人想象的不同，并不是只有硬件设备才有驱动程序，很多软件设备为了实现特殊的功能，也开始带有驱动程序。

因此，在给用户指派安装和卸载设备驱动的权限时一定要谨慎。毕竟大部分时候，设备安装好后很长一段时间内都不需要改动，所以，建议只给管理员用户指派该权限就足够了，而这也是 Windows 的默认做法。

17. 将工作站添加到域

因为该策略只能用于域控制器，因此，在单机和工作组环境下，客户端计算机中的该策略的值是空的。

该策略决定了哪些用户或者用户组可以将计算机加入到域。如果需要让用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的该权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

18. 锁定内存页

该策略的默认值是空的。

该策略决定了哪些用户或者用户组可以用进程将数据保存在物理内存中，而不会被系统分页到硬盘的分页文件中保存，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者用户组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

按照设计，如果运行在 Windows 中的某个程序（可能是系统自带的程序，或者安装的第三方程序）很长一段时间内不使用某些数据，那么 Windows 就会自动将保存在物理内存

中的这些数据写入到硬盘的分页文件（系统盘根目录下一个名为 pagefile.sys 的文件）中，这个过程就叫做“分页”。而一旦程序重新需要这些数据，系统就会自动将分页文件中的数据重新读回物理内存，供程序使用。分页操作可以提升物理内存的使用效率，但与内存相比，硬盘的读写速度实在是太慢了，因此，分页会导致降低系统的整体运行性能。如果希望提高系统性能，最好且最直接的办法是安装更多的物理内存。这个话题和安全无关，因此，本书不准备深入讨论。

19. 拒绝本地登录

该策略的默认值是 Guest 和 HomeGroupUser$。

该策略决定了哪些用户或者用户组可以坐在计算机前进行本地登录。如果需要拒绝某个用户或者用户组本地登录，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望允许某个被拒绝本地登录的用户或者组重新具有本地登录的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

需要注意，如果拒绝了一个用户进行本地登录，但允许该用户通过网络访问这台计算机，那么他可能依然可以通过远程桌面或者远程协助功能登录到这台计算机，或者只通过网络邻居远程访问这台计算机上的共享文件。但对于服务器，如果已经配置好，不再需要本地登录，则可以在服务器中将 Everyone 组添加到该策略中。

20. 拒绝从网络访问这台计算机

该策略的默认值是 Guest。

该策略决定了哪些用户或者用户组无法通过网络访问本机。如果需要拒绝用户或者用户组通过网络访问这台计算机，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望重新允许某个被拒绝从网络登录的用户或者组从网络访问本机，可以在用户或组列表中将其选中，然后单击“删除”按钮。

> **注意** 这里所说的从网络访问本机，可以是远程协助或者远程桌面这样的终端登录，也可以是从网络邻居中访问共享文件这样的远程访问。同时，如果一个用户或组同时出现在“拒绝从网络访问这台计算机”和“从网络访问此计算机”策略中，那么，前者的设置将会覆盖掉后者的设置（在 Windows 中，几乎所有互相冲突的策略、设置等内容，都是被拒绝的设置覆盖掉被允许的设置）。

21. 拒绝以服务身份登录

该策略的默认值是空的。

该策略决定了哪些用户或者用户组无法作为服务登录。如果需要让某个用户或者用户组可以作为服务登录，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组作为服务登录的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

> **注意**　如果一个用户或组同时出现在“拒绝以服务身份登录”和“作为服务登录”策略中，那么前者的设置将会覆盖掉后者的设置。

作为服务登录是什么意思？请运行 services.msc，打开服务控制台，在控制台窗口右侧的窗格中任意双击一个服务，打开其“属性”对话框，随后打开“登录”选项卡，接着可以看到如图 3-8 所示的界面。

图 3-8　在这里可以看到服务的登录身份

请留意“登录身份”选项下的内容。和应用程序的运行一样，服务也是一种特殊作用的应用程序。因此，服务的启动也需要有相应的访问令牌，这样，操作系统才能判断这个服务具有怎样的权限，进而决定它能访问哪些资源。因此，在 Windows 中，有本地系统（Local System）、本地服务（Local Service）和网络服务（Network Service）这三个特殊的账户，这三个账户是专门为各种服务准备的，具有不同的权限，适合不同的服务根据其自身要求用来登录。同时，这三个特殊的系统账户无法用于控制台登录（也就是坐在计算机前进行本地登录，或者通过远程桌面登录）。

然而，有时候却存在另一种情况：可能某个第三方软件或者我们自己的某些应用必须要求以服务的形式运行，这就要求为其准备一个合适的服务账户。而系统自带的这三个服务账户可能无法满足我们的需要，这时候就只能使用自己创建的账户，该账户就需要“作为服务登录”。

22. 拒绝作为批处理作业登录

该策略的默认值是空的。

该策略决定了哪些用户或者用户组无法作为批处理作业登录。如果需要让某个用户或者用户组可以作为批处理作业登录，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的选择用户或组对话框中进行添加；如果希望撤销某个用户或者组作为批处理作业登录的权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

> **注意**　如果一个用户或组同时出现在“拒绝作为批处理作业登录”，以及“作为批处理作业登录”策略中，那么前者的设置将会覆盖掉后者的设置。

作为批处理作业登录是什么意思？其实该策略的作用和“拒绝以服务身份登录”类似，只不过应用到的不是供服务进行登录的账户，而是供批处理任务，也就是计划任务登录的账户。例如，很多有经验的管理员都会自己编写批处理脚本，让计算机在空闲的时候自动执行一些维护任务（例如空闲的时候整理磁盘碎片、查杀病毒或者备份文件等）。然而这就存在一个问题，假设我们需要让计算机在每周三的凌晨 2:00 点整理磁盘碎片，而且创建好了计划任务，难道周二下班之前我们必须使用自己的账户登录到系统才离开吗？这样做是非常危险的。因此，更好的办法是周二下班前注销，但让计划任务在预定的时间自动启动，并运行。

但这样的情况下，计划任务使用什么身份运行？因为身份的不同决定了计划任务获得的访问令牌不同，进而可以进行的操作也就不同。因此，有时候我们可能还需要创建一些专门供批处理脚本或者计划任务使用的账户，这就叫做“作为批处理作业登录”。例如，如图 3-9 所示是在 Windows 7 下打开一个计划任务后看到的结果，请注意其中的“运行任务时，请使用下列用户账户”文本框中显示的内容，这就是在运行该任务时用于“作为批处理作业登录”的账户，如果拒绝该账户作为批处理作业登录，那么除非在该计划运行的时候账户已经登录，否则所有使用该账户运行的计划任务都将无法正常运行。

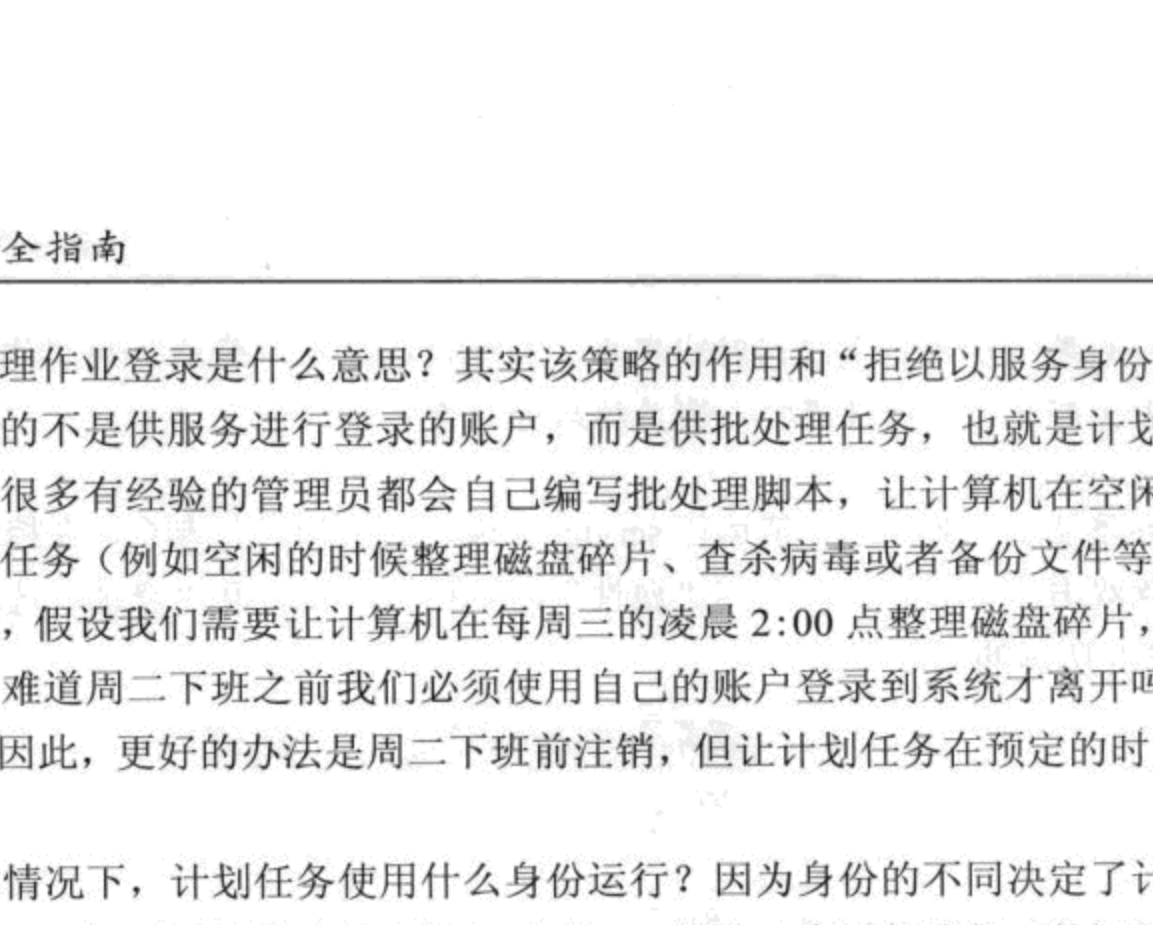


图 3-9　在计划任务中设置的登录账户

23. 配置文件单个进程

该策略的默认值是 Administrators。

该策略决定了哪些用户或者用户组可以用性能监视工具监视非系统进程的性能，注意，

这里所说的监控非系统进程的性能，并不是指性能控制台，而是指通过 WMI 收集数据的操作，也就是说，如果某个程序需要通过 WMI 收集性能数据，那么该程序的访问令牌对应的账户就必须有这个权限。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

24. 配置文件系统性能

该策略的默认值是 Administrators。

和上一条策略类似，该策略决定了哪些用户或者用户组可以用性能监视工具监视系统进程的性能。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

25. 取得文件或其他对象的所有权

该策略的默认值是 Administrators。

该策略决定了哪些用户或者用户组可以获得对象的所有权。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

在本书第 5 章“数据安全”中，将介绍利用 NTFS 权限保护文件和文件夹的安全，其中有很重要的一点，就是对象的所有权。顾名思义，所有权表示了该对象的主人，而主人可以对自己拥有的对象进行任何操作。注意，所有权是可以直接获取的，哪怕一个人并没有该对象的任何访问权限，但只要该用户或者用户组通过本策略具有了获取所有权的权限，那么他就可以将原本不属于自己的对象变成自己的。

因此，设置这条策略时一定要谨慎，尽量不要给其他用户或者组指派这个权限。同时，默认的 Administrators 组建议也不要删除（或者可以从该策略中删除 Administrators 组，但给某个特定的管理员账户指派获取所有权的特权），因为这样在权限设置错误导致对象无法被任何人访问的时候，还可以使用管理员账户进行纠正，而一旦管理员账户没有这个权限了，这个文件就真正无法被访问（甚至删除都不行）。

26. 绕过遍历检查

该策略的默认值是 Administrators、Backup Operators、Everyone、Local Service、Network Service 和 Users。

该策略决定了哪些用户或者用户组可以看到目录中的子文件夹的内容（即使他没有访问的权限），一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权

限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

这个策略是什么意思？假设有一个叫“Folder”的文件夹，其中有一个叫“File”的文件和一个叫“Subfolder”的子文件夹，那么具有该策略指定权限的用户或者用户组即使没有访问 Folder 文件夹的权限，依然可以知道其中有一个叫做“Subfolder”的子文件夹，但不会知道其中有一个叫做“File”的文件。也就是说，可以看到所有子目录的名称，但无法看到其中保存的文件的名称和内容。通常情况下不建议对该策略进行修改，否则可能影响到某些程序的正常使用。

27. 身份验证后模拟客户端

该策略的默认值是 Administrators、Local Service、Network Service，以及 Service。

该策略决定了哪些用户或者用户组运行的程序可以模拟客户端，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

28. 提高计划优先级

该策略的默认值是 Administrators。

该策略决定了哪些用户或者用户组可以使用具有“写入属性”的进程访问另一个进程，以提高分配给另一进程的执行优先级，也就是说，决定了哪些用户或者用户组可以通过任务管理器更改进程的优先级。一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

我们都知道，Windows 是一个多任务操作系统，也就是说，在 Windows 中，可以同时运行多个程序。然而这种“多任务”实际上只是一种由 Windows 让我们造成的感觉，严格地说，在 Windows 中依然是同一时间只能运行一个程序（进程）。那么，为什么我们可以同时运行很多程序？其实，Windows 本身就有很多进程，这些进程也是在同时运行的，这主要依赖了目前速度较高的 CPU，Windows 可以将 CPU 的“能力”分配给所有的程序或者进程，也就是说，在相对于我们来说很短的时间（例如 1 秒）内，CPU 的能力实际上是被轮流使用的，例如程序 A 使用其中的 10 毫秒，程序 B 使用其中的 10 毫秒。因此，计算机依然是在同一时间里执行一个任务，只不过对我们的感觉来说好像多个任务在同时进行，同时互相之间没有影响。

这就带来了另一个问题，不同的任务对 CPU 能力以及其他系统硬件资源的要求是不同的。例如，在玩游戏的时候，系统的后台可能在运行反病毒软件的实时监控功能，在这个

时候可以忍受反病毒软件的“迟钝”，但不能忍受游戏的“迟钝”。而当用反病毒程序扫描硬盘的时候，系统可能还在同时运行网络防火墙的监控程序，这时候可以忍受网络防火墙的“迟钝”，但不能忍受反病毒软件的“迟钝”。

Windows 通过优先级功能决定对不同任务的处理方式。例如，有程序 A 和程序 B 在运行，而且这两个程序对应的进程在默认情况下都具有“普通”优先级，那么 Windows 就会平等对待这两个程序。但如果程序 A 具有“高于标准”的优先级，程序 B 具有“普通”优先级，也就是说，程序 A 的优先级高于程序 B，那么系统会优先满足程序 A 对资源的需求，只有在满足程序 A 的前提下才会尽量满足程序 B 的要求。

如果我们在进行一些需要尽快完成的任务，例如正在给视频文件编码，那么就可以人为地提高编码软件的优先级。其方法如下：

STEP 01 在任务栏的空白处单击鼠标右键，选择“任务管理器”，打开 Windows 任务管理器窗口。

STEP 02 打开任务管理器的“进程”选项卡，找到目标软件对应的进程，并用鼠标右键单击。

STEP 03 在随后出现的菜单中指向“设置优先级”命令，然后选择一个想要使用的优先级（如图 3-10 所示）。

在 Windows 中，共有 6 个不同程度的优先级，这些优先级从高到低分别是：实时、高、高于标准、普通、低于标准和低。通常情况下，大部分系统进程和应用程序的进程优先级都是“标准”。

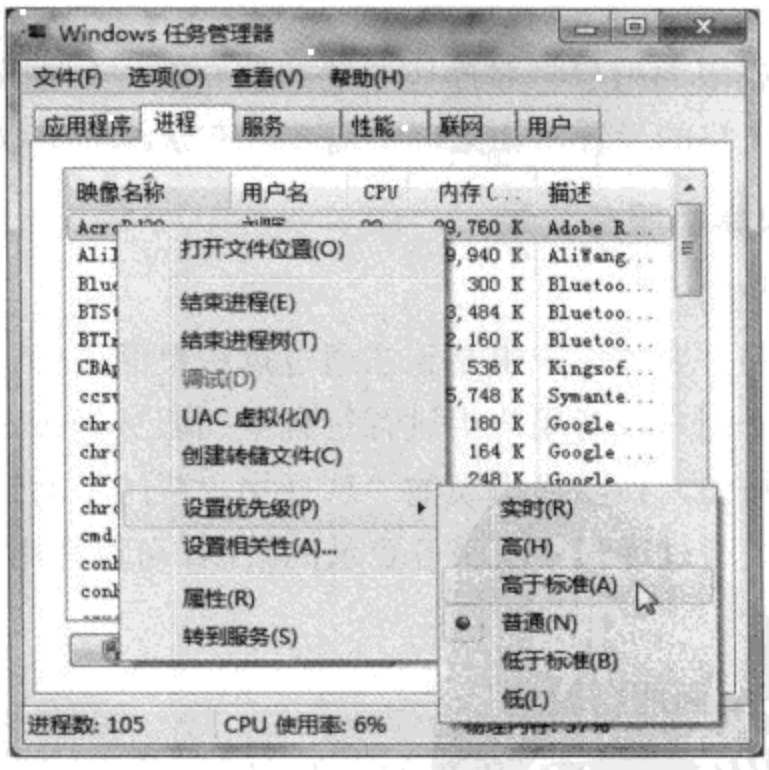


图 3-10　调整进程的优先级

在给 Windows 中的进程调整优先级的时候一定要注意，有些关键系统进程的优先级在默认情况下就不是“普通/标准”，对于这类进程，一般情况下请不要修改其优先级，因为

错误的设置有可能导致系统无法正常工作。注意，如果将某个程序的优先级设置得比较高，而程序突然出现了崩溃或者挂起的现象，就有可能导致整个系统都停止响应，因为如果程序的优先级设置为高于系统进程，那么在这个程序出现错误或者陷入死循环后，系统可能根本没有足够的资源来响应系统或 Windows 资源管理器的要求，无法杀死进程。这时候，除了等待程序恢复正常，也许只能重启（Reset）整个计算机。

29. 替换一个进程级令牌

该策略的默认值是 Local Service 和 Network Service。

该策略决定了哪些用户或者用户组可以让一个服务启动另一个服务，例如，让计划任务服务在特定的条件下启动其他程序或者服务，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

30. 调试程序

该策略的默认值是 Administrators。

该策略决定了哪些用户或者用户组可以将调试程序附加到任何进程或内核，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

要注意，具有这个权限的用户将对操作系统的核心组件具有完整的控制权。因此，一般情况下不建议修改该策略的设置，如果确实需要，在修改的时候也一定要谨慎。

31. 拒绝通过远程桌面服务登录

该策略的默认值是空的。

该策略决定了哪些用户或者用户组是无法通过远程桌面服务（终端服务的新名称）登录的。如果需要拒绝某个用户或者用户组进行远程桌面服务登录，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销对某个用户或者组通过远程桌面服务登录的限制，可以在用户或组列表中将其选中，然后单击“删除”按钮。

32. 允许通过远程桌面服务登录

该策略的默认值是 Administrators 和 Remote Desktop Users。

和上一条策略截然相反，该策略决定了哪些用户或者用户组可以通过远程桌面服务进行登录。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个

用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

33. 同步目录服务数据

该策略的默认值是空的。

该策略决定了哪些用户或者用户组可以对目录服务（最常见的就是 Active Directory）的数据进行同步，因为该策略在一般情况下只适用于具有 Active Directory 的企业网络环境中。因此，在单机和工作组环境下，不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

34. 为进程调整内存配额

该策略的默认值是 Administrators、Local Service 和 Network Service。

该策略决定了哪些用户或者用户组可以对进程可消耗的最大内存进行限制，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

简单地说，具有这个权限的用户可以限制每个进程最多可以使用多少内存。这对于内存数量有限，但又需要运行多个程序的用户来说是非常有用的。要使用这个功能，我们还需要安装 Windows 系统资源管理器（WSRM），这个软件的介绍和下载地址请访问：http://tinyurl.com/yfzdyud。注意，该工具最适合的场合还是运行服务器版 Windows 的计算机，对于运行客户端 Windows 的一般个人计算机，只能安装该工具的客户端对网络上其他安装了该工具的服务器进行管理。因此，个人用户没必要使用。

35. 信任计算机和用户账户可以执行委派

该策略的默认值是空的。

该策略决定了哪些用户或者用户组可以对用户或计算机对象上的账户控制标志进行编辑，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

36. 修改固件环境值

该策略的默认值是 Administrators。

该策略决定了哪些用户或者用户组可以通过应用程序接口或者“系统属性”对话框修改系统环境变量，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具

有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

37. 修改一个对象标签

该策略的默认值是空的。

该策略决定了哪些用户或者用户组可以修改对象（文件、文件夹、注册表键等）的完整性标签，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

为了提升系统安全，在 Windows 7 中增加了一种叫做强制完整性级别检查（MIC）的功能。简单来说，系统会根据实际用途为关键系统文件创建完整性标签，同时其他所有的文件和对象都具有“中级”的完整性级别，而每个进程也有各自的完整性标签。当进程需要修改文件的时候，系统会自动比较进程和文件（对象）的完整性标签，只有进程的完整性级别大于或者等于对象的完整性级别，进程才可以写入对象；如果小于对象的完整性级别，则只能读取，不能写入。而“修改一个对象标签”策略就控制了可以修改对象的完整性标签的特权。

38. 以操作系统方式执行

该策略的默认值是空的。

该策略决定了在没有经过身份验证的情况下，进程可以模拟哪些用户或者用户组的身份以访问与该用户相同的本地资源的访问权限，一般情况下不建议修改这里的设置。如果需要让进程模拟某些用户或者用户组，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望禁止对某个用户或者组的访问，可以在用户或组列表中将其选中，然后单击“删除”按钮。

> **注意** 该策略主要用于包含了 Windows 2000 Server 以及 Windows NT 4 Server 的企业网络，主要用途是提供向下兼容性。对于运行了 Windows Server 2003，以及更新版本的企业网络，没必要配置该策略。

39. 允许本地登录

该策略的默认值是 Administrators、Backup Operators、Guest 和 Users。

该策略决定了哪些用户或者用户组可以进行本地登录。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

> **注意**　对该策略的配置既不会影响到用户通过远程桌面功能进行登录，也不会影响到通过网上邻居访问共享文件或打印机。

40. 增加进程工作集

该策略的默认值是 Users。

该策略决定了哪些用户或者用户组可以修改进程工作集的大小设置，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

所谓“工作集”，是指物理内存中当前进程可见的内容页面集。简单地说，它代表了进程对物理内存的使用情况。

41. 执行卷维护任务

该策略的默认值是 Administrators。

该策略决定了哪些用户或者用户组可以运行卷维护任务（例如，磁盘碎片整理程序或者磁盘管理控制台等）。因为具有该权限后可能会危及文件系统安全，因此，建议一般情况下不要修改该策略的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

42. 作为服务登录

该策略的默认值是空的。

该策略决定了哪些用户或者用户组可以将进程作为服务进行注册，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

> **注意**　该服务的用户类似于“拒绝以服务身份登录”策略，只不过这两条策略的作用正好互斥。有关它们更详细的信息还可以参考上文“拒绝以服务身份登录”一节。

43. 作为批处理作业登录

该策略的默认值是 Administrators 和 Backup Operators。

该策略决定了哪些用户或者用户组可以通过批处理队列工具登录，主要用于计划任务程序，一般情况下不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，

可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

> **注意** 该服务的用户类似于“拒绝作为批处理作业登录”策略，只不过这两条策略的作用正好互斥。有关它们更详细的信息，还可以参考上文中“拒绝作为批处理作业登录”的相关内容。

44. 作为受信任的呼叫方访问凭据管理器

该策略的默认值是空的。

该策略主要用于备份和还原凭据管理器，通常只有系统的 Winlogon 进程需要该特权，而用户不需要直接使用该特权。因此，不建议修改这里的设置。如果需要让其他用户或者用户组具有该权限，可以打开该策略，然后单击“添加用户或组”按钮，在随后出现的“选择用户或组”对话框中进行添加；如果希望撤销某个用户或者组的这个权限，可以在用户或组列表中将其选中，然后单击“删除”按钮。

3.2.3 安全选项

除了可以通过上一节提到的策略给不同的用户或者组指派权限外，还可以在“安全选项”节点下，针对系统的全局安全设置进行调整。这里列举的策略都是很关键的，在经过恰当的设置后，可以极大地提高系统的安全性，但如果设置错误，则有可能影响系统安全，甚至影响正常的使用。

因此，如果你不清楚一个策略是否需要，或者不了解策略的详细作用，最好不要修改设置，使用默认值即可。

1. DCOM：使用安全描述符定义语言（SDDL）语法的计算机启动限制

该策略的默认值是“没有定义”。

该策略可以用安全描述符定义语言（Security Descriptor Definition Language，SDDL）对计算机的 DCOM 应用程序启动和激活等操作进行限制。简单地说，可以通过该策略设置允许哪些用户或者用户组通过远程或本地的方式访问启动或者使用本机上的 DCOM 应用程序。

通常情况下，该策略使用默认设置即可。但如果需要修改，可以按照下列方法对其进行配置：

STEP 01 双击该策略，打开“属性”对话框，并单击“编辑安全设置”按钮。

STEP 02 在如图 3-11 所示的“访问权限”对话框中，已经默认预置了 4 个用户和组。

STEP 03 这里的设置方法和设置 NTFS 访问权限基本相同，只要选中想要设置的用户或者组，然后根据实际需要选择对应权限的“允许”或“拒绝”权限即可。

图 3-11　为不同的用户和组设置 DCOM 程序的启动和激活权限

STEP 04 如果要设置的用户或者组没有出现在列表中，可以单击“添加”按钮，在随后出现的“选择用户或组”对话框中选择要设置的用户或者组。

2. Microsoft 网络服务器：登录时间过期后断开与客户端的连接

该策略的默认值是“已启用”。

该策略主要用于带有 Active Directory 的企业网络中，因为在 Active Directory 中，管理员可以设置用户或者用户组的允许登录时间，只有在允许的时间内，该账户才被允许登录，同时该策略只影响 SMB（Server Message Block，服务器消息块）连接，也就是我们平时使用网上邻居访问网络中其他计算机上的共享文件或共享打印机时使用的协议。

既然可以在 Active Directory 中限制用户或者用户组登录的时间，那么，如果一个用户允许在每天早上 8 点到 9 点之间登录，他在 8 点半登录并打开了对方计算机上的共享文件后，如果一直没有关闭这个文件的访问连接，过了 9 点应该怎样处理？如果启用该策略，只要一到 9 点，该登录打开的连接都会被服务器自动断开；如果没有启用该策略，那么这个用户依然可以使用已经创建的连接，并且在他注销之前一直可以使用，只是无法创建新的连接（打开新的文件）。

3. Microsoft 网络服务器：对通信进行数字签名（如果客户端允许）

该策略的默认值是“已禁用”。

接下来要介绍几个与网络通信的数字签名和数字加密相关的策略，那么加密和签名到底有什么区别？下面逐一进行说明。

所谓签名，主要用途是证明通信的实际来源，以及在传输过程中是否被篡改。例如，如果主机 A 和主机 C 需要通信，但链路要通过主机 B 实现，其中的主机 B 起到了一个类似“转发”的作用，如果主机 B 上安装有特殊的软件，可能会篡改主机 A 和主机 C 之间的

通信数据。而一旦主机 A 和主机 C 之间的通信被数字签名了，那么只要通信数据被篡改，这两台系统立刻就会知道，同时数字签名技术还可以证实来源的准确性。例如，假设主机 B 冒充主机 A 给主机 C 发送数据，因为无法伪造主机 A 的数字签名，因此，主机 C 只要看到数据的数字签名，就可以知道这些数据是否来自真正的主机 A。

而加密的主要目的是为了防止窃听。例如，主机 A 要通过主机 B 发送数据给主机 C，一旦进行通信加密，主机 A 发出的数据将会使用复杂的算法进行加密，同时，只有主机 C 可以解密并查看其内容。这样主机 B 虽然可以“转发”数据，但因为无法解密，因此，不会知道数据的实际内容。

在这里需要注意，虽然这几条策略中都提到了“客户端”和“服务器”的概念，但这并不是用于区别 Windows 的版本。这里的“服务器”并不仅仅指安装了服务器版 Windows 的计算机，“客户端”也并不仅仅指安装了客户端版本 Windows 的计算机。这里所说的“客户端”和“服务器”是通过在连接中的实际作用来区分的。假设一台运行 Windows Server 2008 的计算机需要访问一台运行 Windows 7 的计算机上的共享文件，那么在这个活动中，“服务器”是运行 Windows 7 的，提供了文件访问服务的计算机；而“客户端”反而是运行 Windows Server 2008 的，需要访问其他计算机上文件服务的计算机。

另外需要注意的一点，这条策略和下文要介绍的“Microsoft 网络服务器”和“Microsoft 网络客户端”策略都只是针对在局域网环境内使用的 SMB 协议的，也就是说，只适用于通过网上邻居访问局域网的文件共享或打印机共享。

该策略可以根据客户端的配置决定是否对服务器端的 SMB 组件进行数字签名。启用该策略后，在进行过网络验证后，如果经过协商，服务器发现客户端可以接受数字签名，就会自动将 SMB 数据包进行数字签名。

4. Microsoft 网络服务器：对通信进行数字签名（始终）

该策略的默认值是“已禁用”。

虽然该策略也可以决定是否对服务器端的 SMB 组件进行数字签名，不过决定权在服务器（上一条策略的决定权在客户端）。在启用该策略后，无论客户端是否可以接受数字签名，服务器上发出的数据都会进行签名。

5. Microsoft 网络服务器：服务器 SPN 目标名称验证级别

该策略的默认值是“没有定义”。

该策略决定了具有共享文件夹或打印机的计算机对客户端计算机使用 SMB 协议创建的会话所提供的服务主体名称（SPN）的验证方式。

简单地说，在使用 SMB 协议创建网络会话时，SMB 服务器端可以对 SMB 客户端的服务器主体名称（Service Principal Name，SPN）进行验证，这主要是为了防范 SMB 中继攻击。SPN 是指服务实例所具有的唯一的标识信息（这一点可以理解为 Windows 中账户的 SID）。如果客户端的某个服务具有多个实例，那么每个实例也将有唯一的 SPN。有关 SPN

的详细介绍，可参考 http://tinyurl.com/yer8fz8。

对于该策略，如果不需要验证客户端的 SPN，可以设置为“关闭”；如果希望在客户端提供 SPN 的时候对该 SPN 进行验证，并只有验证到匹配的结果后才允许通信，则可以选择“由客户端提供时接受”，但这种情况下，SPN 并不是强制要求的，如果客户端不提供 SPN，则可直接建立通信；如果强制要求客户端提供 SPN，并且只有在验证到匹配的结果后才允许通信，则可以选择“客户端需要”，这种情况下，客户端如果不提供 SPN，或者提供了不匹配的 SPN，都将无法通信。

6. Microsoft 网络服务器：暂停会话前所需的空闲时间数

该策略的默认值是 15 分钟。

该策略决定了 SMB 会话在不活动多长时间后会自动被服务器暂停。简单地说，当客户端打开服务器上的一个共享文件，但在一定长度的时间内没有访问其他文件后，该会话就会被服务器暂停（也叫做挂起），这个时间长度是由本策略决定的。当一个会话被暂停后，如果需要重新恢复到可访问状态，需要重新建立会话。

7. Microsoft 网络客户端：对通信进行数字签名（如果服务器允许）

该策略的默认值是“已启用”。

该策略的作用和上文介绍的“Microsoft 网络服务器：对通信进行数字签名（如果客户端允许）”的作用类似，只不过在本策略中，进行数字签名的是客户端的 SMB 组件，同时决定权在服务器端。也就是说，如果启用该策略，那么只要服务器端可以接受对 SMB 通信进行数字签名，客户端的 SMB 组件就会被自动签名。

8. Microsoft 网络客户端：对通信进行数字签名（始终）

该策略的默认值是“已禁用”。

该策略的作用和上文介绍的“Microsoft 网络服务器：对通信进行数字签名（始终）”的作用类似，只不过在本策略中，被签名的是客户端 SMB 组件，且服务器端无论是否可以接受，都会被签名。

9. Microsoft 网络客户端：将未加密的密码发送到第三方 SMB 服务器

该策略的默认设置是“已禁用”。

除了 Windows 操作系统可以使用 SMB 通信外，还有很多其他操作系统可以实现，例如，在 Linux 系统中安装 Samba 软件后，就可以让 Linux 操作系统访问 Windows 的共享文件，同时，Windows 也可以访问 Linux 中的共享文件。这类非 Windows 的兼容 SMB 协议的应用就叫做第三方 SMB 服务器。通常情况下，为了保证安全，在进行 SMB 通信之前需要对用户的身份进行验证，而验证信息（用户名和密码等信息）是被加密后传输的，这样可以保证密码或者其他重要信息不被外泄。然而并非所有的第三方 SMB 服务器都支持在验证身份的时候对密码进行加密。因此，该策略决定了如果要访问的第三方 SMB 服务器无法

接受被加密的密码信息，那么是否将未加密的密码发送出去。

通常情况下，建议该策略保持默认值，也就是将其禁用。而一旦网络中确实有不支持加密验证的 SMB 服务器，同时又必须使用该服务器，则可以按照实际情况将其启用。只不过这样做有可能导致密码外泄。

10. 关机：清除虚拟内存页面文件

该策略的默认值是“已禁用”。

对 Windows 有一些基本了解的人一定知道，Windows 中用了一种叫做“虚拟内存/分页文件”的技术，可以将已经载入到物理内存中，但较长时间没有被使用的数据重新写入硬盘的一个特殊文件中，而一旦系统或者软件重新需要该数据，数据就会被从这个特殊的文件中重新读回物理内存。这种操作叫做分页，硬盘上，这个特殊的文件就叫做分页文件，有时候也被叫做页面文件。

分页是 Windows 中一项十分常见的操作，不管技术如何进步，到了大容量内存非常普及的今天，该功能依然没有被取消。分页操作可以提高数量有限的物理内存的使用效率，让系统和程序能够更加平滑地同时运行。然而这里存在一个问题：如果我们在 Windows 中处理了一些机密数据，在处理过程中，这些数据很可能曾经被 Windows 分页到硬盘上。当处理完毕，并将机密文件妥善保管好之后，这个文件中的某些信息可能依然存在于分页文件中，有时甚至可能会在里面保存好多天。虽然无法直接在 Windows 下使用常见的软件读取分页文件中的内容，不过确实有程序可以对分页文件进行分析，并从中读取数据。因此，如果计算机需要用于处理机密信息，那么最安全的办法就是启用该策略。这样，在关机的时候，Windows 会自动将分页文件清理掉，并在下次开机的时候重新创建。

另外需要注意一点，启用该策略后会极大地延长 Windows 的关闭时间，因为启用该策略后，Windows 在关机的时候并不是简单地在系统分区的主文件分配表中将分页文件标记为“已删除”（一般情况下，当我们在 Windows 下删除文件的时候，Windows 就是这样做的。这样做虽然速度快，但很不可靠，因为反删除软件可以顺利地找回这样删除的文件），而是用随机数据将分页文件占用的硬盘扇区全部填充。这样做即使用反删除软件也将无法找回分页文件中的数据。因此，这会降低关机速度，尤其是如果分页文件设置得比较大的时候。

关于文件的安全删除和反删除，请参考本书 5.6 节文件的彻底删除和反删除中的相关内容。

11. 关机：允许系统在未登录的情况下关闭

该策略的默认值是“已启用”。

在上文中介绍“关闭系统”策略的时候曾经提起过，很多专用的 Windows 系统（例如服务器）都是不能被随意关闭的，因此，在这类系统上可以通过策略决定允许哪些用户或者用户组关闭。该策略的作用是决定当计算机已经启动，但没有用户登录的时候，是否在

欢迎屏幕上显示关机按钮，并允许直接关机。

该策略默认情况下是被启用的，这样，当启动 Windows 到欢迎屏幕，还没有任何用户登录的情况下，Windows 将会显示关闭按钮，供我们在登录之前关闭计算机。一旦禁用该策略，那么在欢迎屏幕上如果没有任何用户已经登录，将找不到关闭选项。当然，此时依然可以通过拔掉电源线的方法“关机”，但至少无法从 Windows 自身提供的选项将系统安全关闭。

这个策略同样主要是适用于专用的计算机，例如服务器。因为很多服务器都是要运行后台服务的，即使没有用户登录，这些服务也可以正常使用。因此，在服务器上最好启用该策略，这样别人就无法正常关机。如果真需要关机，就只能使用具有关机权限的账户登录系统，然后关闭。

12. 恢复控制台：允许软盘复制并访问所有的驱动器和所有的文件夹

该策略的默认值是“已禁用”。

默认情况下，当进入到故障恢复控制台后，只能访问有限的几个系统目录（虽然此时是使用管理员账户登录的），这主要是为了安全，因为故障恢复控制台的主要作用是为了在操作系统崩溃，甚至连安全模式都无法进入的情况下，提供一个字符界面供我们使用命令行程序解决问题。因此，默认情况下，该功能限制了只能访问到系统目录，毕竟解决系统问题只需要访问这几个目录就足够了。同时，为了保证保存在本地硬盘上文件的安全，默认情况下，在故障恢复控制台中无法将本地硬盘上的文件复制到可移动存储设备。然而，只要启用该策略，所有这些限制都将被取消。

13. 恢复控制台：允许自动管理登录

该策略的默认值是“已禁用”。

默认情况下，当试图进入到故障恢复控制台环境下之前，必须使用系统内建的 Administrator 账户登录才能继续操作。启用该策略后，只要选择进入故障恢复控制台，不需要登录即可直接使用。通常不建议启用该选项，毕竟需要登录还可以进一步增强安全性。

14. 交互式登录：不显示最后的用户名

该策略的默认值是“已禁用”。

为了方便使用，默认情况下，Windows 会在“Windows 登录”对话框的“用户名”一栏显示上一次登录用户的用户名。这样，如果该用户下次继续登录，只要输入密码即可，简化了登录过程。然而这样做也容易造成安全隐患，因为任何能够看到登录界面的人都会知道至少一个本机上的有效账户的名称，进而可能会通过猜测或者暴力破解的方法攻击系统。

如果启用该策略，“Windows 登录”对话框中就不会显示上一次登录账户的用户名。每个用户在登录的时候都必须输入自己的用户名和密码。

如果需要进一步的安全，可以考虑启用该策略。注意，该功能对于 Windows 7 的欢迎

屏幕无效。

15. 交互式登录：试图登录的用户的消息标题

该策略的默认值是空的。

通过配置该策略，和下面的“交互式登录：试图登录的用户的消息文本”配合，可以让用户在登录系统之前看到一个提示信息。例如，可以在提示信息中声明一些公司计算机的安全使用注意事项，或者发布通知。

该策略决定了用户登录时看到的消息的标题，也就是“消息”对话框的标题栏显示的内容。

16. 交互式登录：试图登录的用户的消息文本

该策略的默认值是空的。

和上面一条策略的作用类似，不过该策略设定的是用户登录时看到的消息的正文内容。

17. 交互式登录：锁定会话时显示用户信息

该策略的默认值是空的。

这个策略决定了在域环境中，当将计算机锁定后，计算机的屏幕上显示有关用户的哪些信息。如果希望显示完整的用户信息，例如账户名、域名等，可以选择“用户显示名称、域名和用户名”；或者也可以根据需要选择“仅用户显示名称”或“不显示用户信息”。

对于安全性要求较高的场合，通常建议使用“不显示用户信息”，毕竟向无关人员泄露的信息越少（哪怕是看似无关紧要的信息），也就越安全。

18. 交互式登录：提示用户在过期之前更改密码

该策略的默认值是“14 天”。

这条策略决定了在用户的密码快要过期的时候，Windows 在过期前多少天开始提示用户更改。例如，默认设置的是 14 天，当一个用户的密码还剩 14 天就要过期的时候，这个用户登录后就能看到一个建议立刻更改密码的提示信息。同时，在过期前，该用户每次登录的时候都会看到同样的提醒。

如果没有设置过“密码最长使用期限”策略，该策略就没什么意义。另外，可以根据实际安全需要延长或者缩短提醒的天数。

19. 交互式登录：无须按“Ctrl+Alt+Del”组合键

该策略的默认值是“没有定义”。

在介绍这个策略之前，我们先来了解一下为什么一定要按“Ctrl+Alt+Del”组合键之后才输入密码并进行登录。假设有这样一种情况：如果有人编写了一个程序，可以模仿 Windows 的登录界面，并且提供了完全一致的“登录”对话框，还设置这个程序全屏运行覆盖掉屏幕上的其他内容。那么，一旦这样的程序在计算机上运行，这台计算机的用户就

很容易被蒙骗，在这个程序伪造的“登录”对话框中输入自己的用户名和密码。该程序一旦截获了用户名和密码，就可以将密码发送出去。因此，在安全的环境下，最好在登录前要求按下“Ctrl+Alt+Del”组合键。

“Ctrl+Alt+Del”组合键是 Windows 中的一个特殊的组合键，通常可以实现一些很重要的功能。例如，Windows 9x 时代的任务管理器和热启动，以及 Windows 2000/XP/Vista/7 时代的任务管理器和 Windows 安全界面。

下面以实例来说明该策略的用法。对于 Windows 7，在没有账户登录的情况下：

如果不设置该策略，或设置为“启用”的情况下，如果当前没有用户登录，那么在欢迎屏幕上会直接看到本机所有账户的列表，只要选中一个账户的图片，并输入密码，即可登录。

如果禁用该策略，在欢迎屏幕上首先会看到一则消息要求我们按下“Ctrl+Alt+Del”组合键（如图 3-12 所示），随后才可以看到账户列表。如果需要登录的界面是软件模拟出来的，这表示当前已经有用户登录了，并且运行了软件，如果这时候按下“Ctrl+Alt+Del”组合键，出现的将会是“Windows 安全”界面（如图 3-13 所示）。也就是说，可能会有恶意软件模拟出图 3-12 的界面来诱骗用户输入密码。但如果图 3-12 是恶意软件模拟出来的，在按下“Ctrl+Alt+Del”组合键后，并不会看到登录界面，而是直接看到图 3-13 所示的内容。因此，只要能事先给用户做好培训，如果用户打算登录的时候按下“Ctrl+Alt+Del”组合键没有看到预期的账户列表，就表示有问题，用户没有地方可以输入自己的密码，同时也就保证了用户密码的安全。

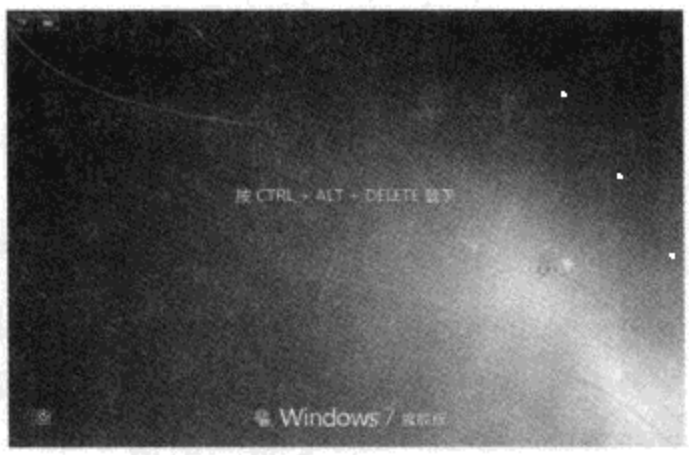


图 3-12　要求按下组合键才能登录

图 3-13　Windows 安全界面

注意　Windows 对策略的“否定”描述。例如，当前这条策略叫做“无须按 Ctrl+Alt+Del”组合键，策略的含义本身就是否定的，这意味着，如果启用该策略，就“不需要”按（正负得负）；如果禁用该策略，就“需要”按（负负得正）。但如果这条策略叫做“需要按 Ctrl+Alt+Del 组合键”（事实上并没有这样的策略，这只是假设出来用于说明问题），启用该策略的时候则“需要”按，而禁用该策略反而就“不需要”按。在 Windows 中有很多策略的名称是“肯定”的，而也有不少的名称是“否定”的，在设置的时候一定要注意区分。

20. 交互式登录：需要域控制器身份验证以对工作站进行解锁

该策略的默认设置是“已禁用”。

这条策略主要用于域环境中。因为和单机以及工作组环境不同，在单机或工作组环境下，用户的登录信息保存在本机的 SAM 数据库中，登录 Windows 的时候，用户输入的用户名和密码是在本机进行验证的；而在域环境下，域账户的登录信息保存在域控制器上，用户登录 Windows 的时候，输入的用户名和密码是在域控制器上进行验证的。这就带来了一个问题，如果是笔记本电脑加入了域，在公司里可以连接到域控制器，自然就可以成功地验证并登录。但如果这台笔记本被带出公司了，例如到了客户的公司里，或者员工拿着笔记本电脑回家，因为没法连接到域控制器，这是否意味着用户无法登录？

为了避免这种情况，默认的设置下，当一个域用户成功登录后，本机会将用户的凭据信息缓存到本地。这样，如果暂时无法连接到域控制器，用户还可以使用本地缓存的凭据信息判断用户是否是合法用户，并决定是否允许登录。这样的默认设置增加了易用性，但降低了安全性。毕竟客户端保存了用户的凭据信息，而这些信息有可能随着客户端离开公司的范围。

为了避免域用户的凭据信息被滥用，可以启用该策略，这样用户试图登录或者解锁计算机的时候，本机就必须能够连接到域控制器，并进行验证。同时，本机不再保存用户凭据的缓存。但如果因为网络故障或者用户出差，无法连接到域控制器，启用该策略将导致计算机无法使用。

因此，请根据实际需要配置该策略。例如，可以统一对所有的笔记本计算机禁用该策略，但同时对所有的台式机启用该策略。

21. 交互式登录：需要智能卡

该策略的默认设置是“已禁用”。

在上文中曾介绍过如何创建安全的密码，并且密码需要定期更换等。这些措施虽然说起来简单，但实际执行的时候总会遇到各种问题，毕竟人都是有惰性的，同时，好密码也很难记忆。为了避免密码导致的安全问题，现在很多大企业已经在考虑使用其他方式取代传统的密码，例如智能卡、指纹或者虹膜等生物特征识别，其中智能卡的使用最常见。

智能卡就像普通的信用卡，其中有一块芯片存储了用户的登录凭据信息。在部署了智能卡的企业中，用户只需要将自己的智能卡插入计算机上的读卡器中，用户名和密码的输入工作就由智能卡代劳了。因为不需要用户记忆密码，因此，智能卡比传统的密码更安全，还不用担心密码遗忘，就算智能卡丢失或者被盗，管理员也可以在第一时间撤销该智能卡对应的凭据信息，这样别人就算得到智能卡，也无法使用。

该策略决定了是否允许除了智能卡外的其他方式进行验证。如果禁用该策略，那么除了使用智能卡，用户依然可以使用传统的密码方式来登录（只要企业网络中依然保留了密码验证的方式）；如果启用该策略，就只能使用智能卡登录。

22. 交互式登录：之前登录到缓存的次数（域控制器不可用时）

该策略的默认设置是“10 登录”。

在“交互式登录：需要域控制器身份验证以对工作站进行解锁”策略的介绍中曾经提到过，默认情况下，Windows 会将域账户的凭据信息缓存起来，以便在无法联系域控制器的时候进行验证。该策略就决定了 Windows 缓存多少个登录凭据，它可用的值是介于 0～50 的整数，如果设置为 0，将不缓存凭据；如果设置为超过 50 的整数，那么，Windows 最多只缓存 50 个登录凭据。

23. 交互式登录：智能卡移除行为

该策略的默认值是“无操作”。

在上文对“交互式登录：需要智能卡”策略的介绍中，曾经提到过，为了增强安全性能，很多企业都部署了智能卡。在需要的时候，只要将自己的智能卡插入到读卡器中，就可以直接登录到 Windows。该策略决定了在成功登录后，如果将智能卡从读卡器中拔出来，Windows 可以采取的操作，例如，可以选择“锁定工作站”、“强制注销”，从 Windows Vista 开始还增加了一个“如果为远程终端服务会话，则断开连接”选项，适用于异地办公的员工。

对于该策略，建议选择“锁定工作站”，这样用户在登录后，如果需要暂时离开自己的计算机，则可以直接将智能卡拔下来，这样计算机会自动锁定。当用户回来后，只要插入智能卡，就可以继续处理离开前的工作。

24. 设备：防止用户安装打印机驱动程序

该策略的默认设置是“已禁用”。

这条策略只对网络打印机有效。我们可以将打印机在网络上共享出来，这样别人如果需要，就可以直接将文档从自己的计算机上通过网络发送给共享的打印机进行打印。然而，和本地打印机一样，要使用网络打印机，必须在本地计算机上安装这台打印机的驱动程序。而该策略就是用于决定是否允许用户安装网络打印机的驱动程序。这条策略不会影响 Administrators 和 Power Users 组的用户。

如果启用该策略，就只有管理员可以给本机安装网络打印机的驱动；如果禁用该策略，那么任何权限的账户都将可以安装网络打印机的驱动。

25. 设备：将 CD-ROM 的访问权限仅限于本地登录的用户

该策略的默认值是空的。

如果启用该策略，就只有从本机进行本地登录的用户可以访问光驱（虽然策略名字中写的是 CD-ROM，实际上该策略可以应用于所有的光存储设备）；如果禁用该策略，那么网络用户也可以访问本机的光存储设备（可以通过网上邻居，或者远程桌面服务）。

26. 设备：将软盘驱动器的访问权限仅限于本地登录的用户

该策略的默认值是空的。

这条策略的含义和上一条类似，可以决定是否允许网络用户使用本机的软驱。

27. 设备：允许对可移动媒体进行格式化并弹出

该策略的默认值是空的。

这个策略决定了谁可以格式化可移动存储介质，以及将其弹出，可选的选项有“管理员”、“Administrators 和 Power Users”，以及“Administrators 和 Interactive Users”。这里简单介绍一下 Interactive Users，这是指通过交互式登录的方式登录到本机的用户。简单地说，就是指在本机前登录的用户。

28. 设备：允许在未登录的情况下弹出

该策略的默认值是“已启用”。

这条策略决定了是否允许在没有任何用户登录的情况下，将连接到扩展坞的便携式计算机从扩展坞上脱离。如果启用该策略，则在没有用户登录的情况下，只要扩展坞上带有硬件形式的弹出按钮，就可以用它直接弹出计算机。如果禁用该策略，用户就必须使用具有“从扩展坞中移除计算机”权限的账户登录系统才能移除计算机。

29. 审核：对备份和还原权限的使用进行审核

该策略的默认值是“已禁用”。

在 3.2.1 节“审核策略”中已经介绍过与审核策略有关的内容。该策略决定了是否对备份和还原操作进行审核。简单地说，如果启用该策略，那么备份和还原操作就会被记录到审核日志中；如果禁用该策略，即使启用了审核，有关备份和还原的操作也不会被记录。

30. 审核：对全局系统对象的访问进行审核

该策略的默认值是“已禁用”。

该策略决定了是否对全局系统对象的访问进行审核。注意：该策略对我们一般的审核操作没什么用，启用该策略后会生成大量用不到的审核日志，而这些日志通常都是开发人员所关心的。因此，一般情况下，就算启用审核，也只需要按照 3.2.1 节“审核策略”中介绍的方法设置审核，而不需要通过该策略启用全局系统对象访问的审核。

31. 审核：强制审核策略子类别设置（Windows Vista 或更高版本）替代审核策略类别设置

该策略的默认值是空的。

在 Windows 7 下查看审核策略的日志时可以发现，与老版本 Windows 相比，Windows 7 的审核策略日志更加详细，因为其中增加了很多子类别，方便我们更直观地找到自己需要关注的日志内容。然而这些新增的子类别只适合 Windows Vista 以上的系统。

如果企业管理员需要同时管理 Windows 7 和 Windows XP 计算机的审核策略日志，为了提供向下兼容性，禁用该策略后就可以避免让 Windows 7 的审核策略日志启用子类别功能。但如果只是管理 Windows Vista/7 的审核策略日志，不管理 Windows XP 或更老的系统，

为了提高易用性，可以启用该策略。

32. 审核：如果无法记录安全审核则立即关闭系统

该策略的默认值是“已禁用”。

在上文介绍审核策略的时候就已经提到过，在启用审核后，取决于审核策略的设置，以及要审核的对象的访问情况，系统中可能会生成大量审核日志记录。如果记录已经满了，那么在该策略的默认设置下，新的审核日志将无法保存。在某些情况下，这是一种不安全的做法，因为管理员无法了解对对象的访问情况。因此，我们可以考虑启用该策略，这样一旦日志满了，非管理员用户登录系统的时候就会看到“STOP:C0000244”错误信息，无法登录系统，同时系统会自动关闭。这时候必须由管理员登录系统，将老的日志记录进行存档或者清理，这样其他用户才可以登录。

启用该策略的时候一定要小心，因为一旦启用，如果我们没能及时清理日志记录的时候，可能会导致用户无法正常使用。因此，在启用该策略后，我们还可以根据需要对事件查看器进行一些设置。

对于 Windows 7，请这样操作：

STEP 01 在“计算机”上单击鼠标右键，选择“管理”，打开计算机管理控制台。

STEP 02 在计算机管理控制台窗口左侧的控制台树中依次展开“计算机管理”→“系统工具”→“事件查看器”→“Windows 日志”→“安全”。

STEP 03 在“安全”节点上单击鼠标右键，选择“属性”，打开“安全性属性”对话框，如图 3-14 所示。

图 3-14　Windows 7 的日志属性对话框

STEP 04 “日志最大大小”选项决定了“安全”日志可以用于保存日志记录的硬盘空间的最大值。对于安全性日志，默认的最大值是 20 480KB，基本上已经可以满足一般情况下的使用。但如果需要审核的对象比较多，也可以根据实际情况调整该日志的最大值设置。

STEP 05 在“达到事件日志最大大小时”选项下可以看到三个选项，这些选项决定了当日志满了后系统要采取的操作：

- **按需要覆盖事件（旧事件优先）** 如果选择该选项，一旦日志满了，新的事件将覆盖最老的事件。
- **日志满时将其存档，不覆盖事件** 在日志满了后，将老的事件内容存档到其他指定的位置，然后将日志清空。
- **不覆盖事件（手动清除日志）** 如果日志满了，将拒绝接受新的事件，直到管理员手工清理。

STEP 06 如果已经查看了所有的日志事件，需要将这些事件都清除掉，这时候可以在对应的节点（例如，“安全”节点）上单击鼠标右键，选择“清除日志”，接下来，Windows 会使用一个对话框询问我们是否要保存这些事件，我们可以根据实际需要决定是否保存。

33. 网络安全：LAN 管理器身份验证级别

该策略的默认值是空的。

在 3.1.1.1 节“策略介绍”中的“密码必须符合复杂性要求”一段中曾经介绍过，Windows 可以使用几种不同的密码验证机制，这些机制包括 LM、NTLM 以及 NTLMv2，按照排列顺序，这三种机制从左到右，其安全性是递增的。但这里还存在一个问题，不同操作系统对这些验证机制的支持情况各不相同。例如，Windows NT 4 就只支持 LM 验证机制，而 Windows 2000 开始增加对 NTLM 的支持，从 Windows XP 开始则增加了对 NTLMv2 的支持。该策略就是用于设置 Windows 所用的验证机制的。

如果网络中操作系统的种类很单一，例如只有 Windows XP 以上的系统，那么很好解决，只要选择所有操作系统都支持的，同时也是最安全的验证机制就可以了；如果网络中还有更老的 Windows，或者其他操作系统，那么为了兼容这些系统，则必须根据这些系统的实际情况选择使用不那么安全，但兼容性更好的验证机制。

该策略可设置的选项包括：

- **发送 LM 和 NTLM 响应** 使用 LM 和 NTLM 身份验证而不使用 NTLMv2。该设置的兼容性最好，但是安全性最差。
- **发送 LM 和 NTLM 响应 -如果已协商，则使用 NTLMv2 会话安全** 使用 LM 和 NTLM 身份验证，并且如果服务器支持，在经过协商后可以使用 NTLMv2。该设置的兼容性最好，同时安全性有所提高。
- **仅发送 NTLM 响应** 只使用 NTLM，并在服务器支持的前提下使用 NTLMv2。该设置的兼容性一般，但安全性较好。

- **仅发送 NTLMv2 响应**　只使用 NTLMv2。该设置的兼容性很差，安全性很好。
- **仅发送 NTLMv2 响应，拒绝 LM**　只使用 NTLMv2，同时域控制器拒绝 LM，只接受 NTLM 和 NTLMv2。该设置的兼容性一般，安全性较好。
- **仅发送 NTLMv2 响应，拒绝 LM 和 NTLM**　只使用 NTLMv2，同时域控制器拒绝 LM 和 NTLM。该设置的兼容性最差，但安全性最好。

> **注意**　在修改该策略的时候一定要考虑好实际的网络环境，即使所有的客户端都运行了最新的 Windows 系统，也要考虑有什么特殊要求的应用程序，因为错误的设置可能导致系统无法登录，或者程序无法正常运行。

34. 网络安全：LDAP 客户端签名要求

该策略的默认值是“协商签名”。

该策略决定了 LDAP 客户端发出请求的签名方式。可设置的选项有“无”、“协商签名”，以及“需要签名”。

LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）是一种 LDAP 服务器和客户端之间的通信协议。该协议主要用于企业网络中存储数据，可以将其看做是一种“数据库”，对于一般用户，该协议的用途不大。因此，这里不准备详细介绍，我们可以直接保留默认设置。

35. 网络安全：基于 NTLM SSP（包括安全 RPC）服务器的最小会话安全

该策略的默认设置是“要求 128 位加密”。

该协议决定了服务器对于会话安全的等级要求。在 Windows 7 中，可用的选项包括“要求 NTLMv2 会话安全”和“要求 128 位加密”。这些选项的作用分别如下：

- **要求 NTLMv2 会话安全**　限制会话必须使用 NTLMv2 验证机制，否则将无法创建。
- **要求 128 位加密**　限制会话必须使用 128 位强加密，否则将无法创建。

36. 网络安全：基于 NTLM SSP（包括安全 RPC）客户端的最小安全会话

该策略的默认设置是“要求 128 位加密”。

关于该协议，所有可用的选项都和上面的与服务器有关的选项类似，其作用也一样。不同之处在于，上面的协议是从服务器端进行限制的，而这个协议是从客户端进行限制的。

37. 网络安全：配置 Kerberos 允许的加密类型

该策略的默认设置是空的。

该策略可用于设置对于 Kerberos 身份验证协议要使用的加密类型。对于单机和工作组环境，该策略没什么意义，不需要修改配置。

38. 网络安全：限制 NTLM: ××××××

这里有 7 条策略都与 NTLM 的限制有关。同样，这些策略都用于域环境，在单机和工

作组环境下没有什么意义，不需要修改。

39. 网络安全：允许 LocalSystem NULL 会话回退

该策略的默认设置是空的。

当连接到运行 Windowes Vista 或 Windows Server 2008 之前的老版本 Windows 计算机时，以 Local System 身份运行，且使用还原到 NTLM 的 SPNEGO(Negotiate)身份验证方式的服务将使用计算机标识。在 Windows 7 中，如果连接到运行 Windows Server 2008 或 Windows Vista 的计算机，则系统服务将使用计算机标识或 NULL 会话。

当连接 NULL 会话时，将会创建一个由系统生成的会话密钥，该密钥不提供任何保护，但允许应用程序对数据进行签名和加密，而且不会出现错误。当连接计算机标识时，则可支持签名和加密，以便提供数据保护。

该策略决定了使用 Local System 账户运行的服务是否可以为了向后兼容而使用 NULL 会话。若无特殊情况，该策略通常使用默认设置即可。

40. 网络安全：允许本地系统将计算机标识用于 NTLM

该策略的默认设置是空的。

该策略与上一条策略的使用范围是类似的，上一条策略决定了是否允许 Local System 服务使用 NULL 会话，而本策略则决定了是否允许在 NTLM 验证中使用计算机标识。该策略将对计算机的身份验证方式产生影响，因此，如果不是有特殊需要，一般建议不要修改该策略。

41. 网络安全：允许对该计算机的 PKU2U 身份验证请求使用联机标识

该策略的默认设置是空的。

在小型网络环境（非域环境）的 Windows 7 计算机中，我们可以针对每位用户设置文件和打印机的共享，通过使用 Windows 7 新增的家庭组（有关家庭组的详细信息，请参考本书第 7 章）功能，再配合联机 ID 功能，我们甚至可以使用 Windows Live ID 等信息指定共享的访问者，并设定权限。

该功能要求首先安装联机 ID 提供程序，在撰写本书的时候，可以使用 Windows Live ID 作为联机 ID。也就是说，在共享资源并设置权限的时候，不仅可以针对本机的用户名设定权限，而且可以针对别人的 Windows Live ID 来设置。例如，可以允许“PC/User1”对该共享资源具有只读权限，但允许“someone@hotmail.com”对该资源具有读写权限（如图 3-15 所示）。联机 ID 是微软提出的一项开放标准，任何人都可以借助该标准编写自己的联机 ID 提供程序。例如，以后我们也许可以使用 QQ 号码指定访问权限等。

这一功能使用了基于用户到用户的公钥加密（Public Key Cryptography Based User-to-User，PKU2U）协议，而本策略就是用于决定是否使用这一功能的。有关 PKU2U 的详细信息，可参考 http://tinyurl.com/y9w6cxv。

需要注意，该策略并不会影响使用域账户或本地账户登录本机的情况。

42. 网络安全：在登录超过时间后强制注销

该策略的默认值是“已禁用”。

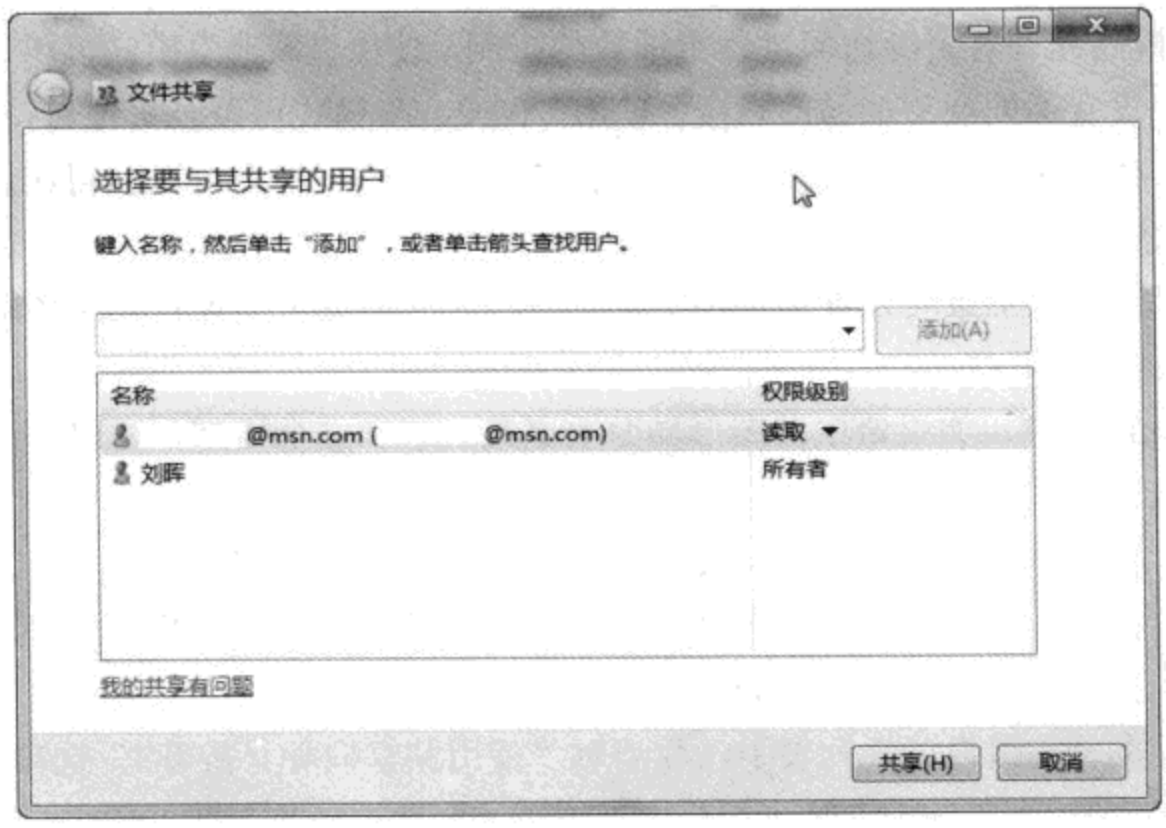


图 3-15　指定共享权限时可直接使用联机 ID

该策略决定了当一个通过 SMB 会话访问的远程用户登录后的时间超出了该账户被允许的有效时间后，系统是否自动将该用户注销。在 3.2.3 节“安全选项”中的“Microsoft 网络服务器：登录时间过期后断开与客户端的连接”一段中介绍的策略和本策略的目的类似，但结果不同。启用“Microsoft 网络服务器：登录时间过期后断开与客户端的连接”这个策略后，一旦超过了允许的登录事件，那么服务器将自动断开会话，但已经建立的会话依然会被维持；而启用了“网络安全：在登录超过时间后强制注销”这个策略后，一旦超过实现，用户不仅会被断开，而且已经建立的会话也会被自动断开。

43. 网络安全：在下一次更改密码时不存储 LAN 管理器哈希值

该策略的默认值是“已启用”。

该策略决定了在下次更改密码的时候是否存储新密码的 LM 哈希值。上文已经说过，LM 是 Windows 支持的所有密码验证机制中安全性最差的。因此，除非需要和老版本 Windows 保持兼容，一般情况下不建议使用该机制。

所以，如果需要考虑和老版本 Windows 的兼容问题，可以禁用该策略；如果不用考虑兼容性问题，或者希望实现更进一步的安全性，可以启用该策略。

44. 网络访问：本地账户的共享和安全模型

该策略的默认值是“经典-对本地用户进行身份验证，不改变其本来身份”。

该策略决定了对使用本地账户进行的网络登录（简单地说，就是通过网上邻居访问本机上的共享文件）时如何进行身份验证。如果设置为“经典”，则使用本地账户凭据的网络登录会使用这些凭据进行身份验证；如果设置为“仅来宾”，则使用本地账户的网络登录将自动映射到 Guest 账户。

“经典”模式允许对资源访问进行更细致的控制，使用“经典”模式可以让同一个资源为不同的用户设置不同类型的访问权限；使用“仅来宾”模式可以公平地对待所有的用户，所有的用户都作为来宾得到身份验证，对于指定资源，这些用户可以获得相同级别的访问权限，即“只读”或“修改”。

除了可以通过安全策略设置共享和安全模型外，还可以通过 Windows 图形界面上提供的选项进行设置。

对于 Windows 7，如果希望在图形界面上更改共享和安全模型，可以禁用共享向导。具体的过程如下：

STEP 01 打开“计算机”窗口，按下键盘上的“Alt”键打开菜单栏。

STEP 02 在“工具”菜单下单击“文件夹选项”，打开“文件夹选项”对话框。

STEP 03 打开“文件夹选项”对话框的查看选项卡。

STEP 04 在“高级设置”列表中，取消对“使用共享向导（推荐）”选项的选择。

> **注意** 在 Windows 7 中启用了共享向导的情况下，可以文件为单位创建共享，而在老版本的 Windows 中只能以文件夹为单位创建共享。这是共享向导的功劳，因此，如果禁用共享向导，将无法继续以文件为单位创建共享。

有关共享的详细信息，请参考本书 7.1 节设置共享的相关内容。

45. 网络访问：不允许 SAM 账户的匿名枚举

该策略的默认设置是“已启用”。

该策略决定了匿名到本机的连接是否可以具有的其他权限。Windows 允许匿名用户执行某些操作，例如枚举域账户名或网络共享名。如果希望匿名用户具有这些权限，可以禁用该策略；如果不允许匿名用户具有这些权限，可以启用该策略。

46. 网络访问：不允许 SAM 账户和共享的匿名枚举

该策略的默认设置是“已禁用”。

该策略决定了是否允许匿名用户枚举 SAM 账户，以及网络共享。如果希望匿名用户有这样的权限，请禁用该策略；如果不希望匿名账户有这样的权限，请启用该策略。

47. 网络访问：不允许存储网络身份验证的密码和凭据

该策略的默认值是“已禁用”。

在使用经典共享模型的情况下，当我们访问网络上的共享文件时，需要输入一个用于

身份验证的凭据（也就是被访问的共享文件所在计算机上的一个本地账户的用户名和密码），只有在输入正确的凭据信息后才允许访问。为了方便使用，默认情况下，Windows 允许我们记住密码。当出现“登录”对话框，并输入用户名和密码后，可以选中“记住密码”选项，这样下次访问该共享资源的时候就不用输入密码了。

然而，这一特性有可能导致安全问题，例如，当我们用一个公用账户登录 Windows 系统并访问共享资源时，无意中可能选中“记住密码”选项。这样当别人使用这个公用账户登录系统后，就可以直接访问共享资源（也许这个人正常情况下并不允许访问这些资源）。为了防止这种问题发生，可以启用该策略，这样在访问网络共享时出现的“登录”对话框中将不会出现记住密码的选项；如果希望允许用户选择记住密码，则可以禁用该选项。

如果在禁用该选项的情况下不小心记住了密码，此时还可以使用本书第 2 章介绍的方法管理本地存储的密码，将不需要的密码删除。

48. 网络访问：将 Everyone 权限应用于匿名用户

该策略的默认设置是“已禁用”。

该策略决定了是否让匿名用户享受到“Everyone”账户的所有特权。在 Windows 中，Everyone 是一个比较特殊的账户，因为这个账户并不代表某个具体的用户，而是用于描述符合某种条件的所有用户。具体来说，Everyone 代表了本机的所有账户，例如 Administrator 是“Everyone”，Guest 是“Everyone”，我们创建的其他本地账户也是“Everyone”。

那么这个策略到底是什么意思？假设希望所有登录到本机的用户都可以访问一个文件夹，最简单的办法就是针对 Everyone 账户设置访问权限，这样就可以将权限直接应用给所有的本地账户。如果有人使用匿名账户连接到本机，而不希望匿名账户访问指派给 Everyone 账户的文件，又该怎样做？只要将该策略禁用即可，因为禁用该策略后，匿名账户将不再是本机的“Everyone”，这样的账户也就不再具有 Everyone 的特权；相反，如果希望匿名用户也可以享受到 Everyone 的特权，只要启用该策略即可。

49. 网络访问：可匿名访问的共享

该策略的默认设置是空的。

该策略决定了匿名用户可以访问本机的哪些共享。如果希望匿名用户可以访问某个共享，只要将该共享的共享名（注意，要添加的是该共享的共享名，而非对应的文件夹名）添加到该策略中即可。

假如禁用了上一条策略，让匿名用户不再具有 Everyone 的特权，而又希望匿名用户可以访问某些共享，就可以将允许其访问的共享添加进来。

50. 网络访问：可匿名访问的命名管道

该策略的默认值是空的。

该策略决定了匿名用户可以访问本机的哪些命名管道。如果希望匿名用户可以访问某

个命名管道，只要将该命名管道的名称添加到该策略中即可。

在介绍命名管道之前，首先要了解什么是管道。简单地说，管道（Pipe）是指用于在进程之间进行通信的一段共享内存，创建管道的进程称为管道服务器，连接到管道的进程为管道客户机。命名管道（Named Pipe）是在管道服务器和一台或多台管道客户机之间进行单向或双向通信的一种方式。对于一般用户，几乎不需要接触这部分概念，本书也不准备过多提及，同时也不建议随意修改该策略的默认设置，以免影响到 Windows 或其他软件的正常使用。

51. 网络访问：可远程访问的注册表路径

该策略的默认值是：

```
System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
```

该策略决定了可以远程访问的注册表路径。如果希望添加可以远程访问的注册表内容，只需要将对应的路径添加到该策略中即可；如果希望停止对某个已经允许远程访问的注册表路径的远程访问，也只需要将其从该策略中删除。

注册表是 Windows 中一个很重要的概念，因为系统的很多重要设置和参数都是保存在注册表中的，我们可以使用注册表编辑器查看和编辑本机的注册表内容。然而很多人不知道的是，注册表除了可以进行本地编辑，还可以在具有权限的情况下编辑远程计算机的注册表。

运行 Regedit 打开注册表编辑器，然后打开编辑器的“文件”菜单，就可以看到“连接网络注册表”命令。通过使用该功能，企业管理员可以坐在自己的计算机前直接连接到局域网内其他计算机的注册表（哪怕这台计算机位于地球的另一边），并直接对其进行编辑、解决问题或者应用某些设置。

然而从安全角度考虑，默认情况下并不能远程访问整个注册表的所有内容。所有可以远程访问的注册表内容就是本策略定义的，我们可以根据实际需要添加或者删除某些内容的远程访问能力。

52. 网络访问：可远程访问的注册表路径和子路径

该策略的默认值是：

```
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
```

```
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog
```

该策略的作用和上一条类似，只不过在 Windows 7 中，利用该策略可以更加细化对注册表的远程访问限制。因为上一条策略在 Windows 中只是用于指定可以远程访问的注册表主键，而该策略可以更加具体地指定可以远程访问的注册表子键。

53. 网络访问：限制对命名管道和共享的匿名访问

该策略的默认值是“已启用”。

该策略决定了是否允许匿名用户访问命名管道和共享。在了解该策略的时候，需要将其与上文提到的“网络访问：可匿名访问的共享”和“网络访问：可匿名访问的命名空间”这两条策略区分开。因为该策略只是用于决定是否允许匿名用户访问命名管道和共享，如果允许访问，那么具体可以访问哪些命名管道和共享则是由前两条策略决定的。

54. 网络访问：允许匿名 SID/名称转换

该策略的默认值是“已禁用”。

该策略决定了匿名用户是否可以通过其他账户的用户名请求获得该账户的 SID，或者通过 SID 获得用户名。在上文已经介绍过，SID 是 Windows 用于区分不同账户的主要途径，而且因为 SID 是唯一的，因此可以说，对系统安全和验证方式都有非常重要的作用。

例如，如果攻击者知道了系统管理员账户的 SID，并且该策略被启用，那么攻击者就可以知道管理员的用户名，进而可以通过猜测或者破解密码等方式非法登录系统。因此，一般情况下，该策略最好保持为默认的禁用设置。

如果网络中有一些老的操作系统，例如 Windows NT 3.x 或者 Windows NT 4，为了正常使用某些功能，我们可能必须启用该策略。因此，建议只有在确实需要的时候才考虑将其启用。

55. 系统对象：非 Windows 子系统不要求区分大小写

该策略的默认设置是“已启用”。

该策略决定了是否对所有的系统对象强制不区分大小写。我们都知道，除了账户密码，Windows 的其他机制几乎都是不区分大小写的，例如，以“A”和“a”为名的文件在 Windows 看来就是同一个文件。然而很多其他操作系统是完全区分大小写的，例如 Linux，在这类系统中，名为“A”和“a”的文件会被看做是两个文件。

如果企业网络中有非 Windows 操作系统，并且是区分大小写的，那么，若要考虑兼容性，我们可能必须让 Windows 也严格区分大小写，这时候就可以禁用该策略。如果不考虑到和非 Windows 系统的兼容性，为了照顾用户的使用习惯，最好还是启用该策略。

56. 系统对象：加强内部系统对象的默认权限（例如，符号链接）

该策略的默认值是“已启用”。

该策略决定了系统对象的默认访问控制列表设置。简单地说，决定了对象的默认权限限制。我们都知道，在安装好 Windows，没有进行任何自定义设置的情况下，很多系统对象就已经具有访问权限限制了，这是微软根据具体对象的作用和需要设置的默认权限。而该策略可以决定默认权限的设置情况。通常没必要更改该策略的设置。

57. 系统加密：将 FIPS 兼容算法用于加密、哈希和签名

该策略的默认设置是“已禁用”。

该策略决定了用于传输层安全性/安全套接字层（TL/SS）安全提供程序是否仅支持面向客户端和服务器（如果适用）的传输层安全（TLS）协议。如果启用该策略，那么，TL/SS 将会使用 Triple DES 加密算法用于 TLS 通信加密，并仅将 Rivest、Shamir 和 Adleman（RSA）公钥算法用于 TLS 密钥交换和身份验证，同时仅将 SHA-1 算法用于 TLS 哈希要求。

FIPS 是美国联邦信息处理标准的英文名称简写，而兼容 FIPS 的算法则是美国政府和某些机构必须使用的。通常情况下，如果不是在美国，或者没有特殊需要，就不必启用该策略。

58. 系统加密：为计算机上存储的用户密钥强制进行强密钥保护

该策略的默认值是空的。

该策略决定了是否将用户保存在计算机上的密钥进行加密保护，如果加密，以后每次使用密钥的时候都必须输入密码。

该策略的可选设置包括：

- 存储和使用新密钥时不需要用户输入。
- 第一次使用密钥时提示用户输入。
- 用户每次使用密钥时必须输入密码。

默认情况下，当将密钥（证书）安装到系统中之后，只要使用当时安装了密钥的账户登录，就可以直接使用该密钥，而不需要额外的身份验证（因为身份验证工作已经在登录 Windows 的时候统一进行了）。有时候也有可能导致安全问题，例如暂时离开计算机，但忘了将计算机锁定，这样别人就可能接触到我们的计算机，进而使用我们的个人密钥进行一些不好的操作。此时可以将该策略设置为“用户每次使用密钥时必须输入密码”选项，这样，就算别人可以使用我们的计算机，也会因为不知道密码而无法使用我们的密钥。

59. 系统设置：将 Windows 可执行文件中的证书规则用于软件限制策略

该策略的默认值是“已禁用”。

该策略决定了在运行可执行文件（.exe 扩展名）的时候是否结合文件自带的数字证书，以及软件限制策略的设置判断是否允许文件运行。软件限制策略是 Windows 中的一个功能，通过该功能，可以借助不同的条件，例如文件名、文件哈希、数字证书等来判断是否允许用户运行这个软件。例如，可以通过软件限制策略决定，带有标示为“Microsoft”的数字证书的软件全部可以运行，或者可以禁止名称为“某某某”的软件运行。如果希望通过数

字证书设置软件限制策略，就必须启用该策略。

注意　关于软件限制策略的详细信息，请参考 3.6 节“软件限制策略”的内容。

60. 系统设置：可选子系统

该策略的默认值是“Posix”。

该策略决定了系统可以使用哪些子系统对某些程序提供支持。对于拥有不同操作系统的企业网络，不同的子系统可以让运行 Windows 的计算机和运行非 Windows 计算机的系统进行交互，或者实现某些功能。通常，对于只运行 Windows 操作系统的网络，或者单机环境，如果不需要考虑和其他非 Windows 的交互问题，可以不配置该策略。

61. 用户账户控制

在 Windows 7 中一共有 10 个名称以“用户账户控制”开头的策略，这些策略可以用于配置 Windows 7 中的用户账户控制功能。关于这些策略，已经在 2.2.2.2 节用策略控制 UAC 中详细介绍过，这里不再复述。

62. 域成员：对安全通道数据进行数字加密（如果可能）

该策略的默认值是“已启用”。

该策略决定了当域成员发现通信的另一端可以支持数字加密的情况下，是否将和对方的安全通道通信数据进行数字加密。通常情况下，这种安全通道用于在域环境下客户端计算机和域控制器进行一些重要的安全验证通信，例如，通过 NTLM 机制验证用户凭据，或者查询 SID 和用户名等。因此，启用该策略可以在一定程度上提高安全性。

当然，该策略所决定的数字加密是在协商的前提下进行的。如果客户端和服务器通过协商，发现可以进行加密，才会真正加密通信；如果通过协商发现其中一方无法接受加密，则不进行加密。因此，启用该策略可以在保证兼容性的前提下尽可能增强安全性。

加密的作用是防止窃听，因为被加密的数据被窃取后，将无法提供解密所需的密钥，从而可以保证数据的安全性。

63. 域成员：对安全通道数据进行数字加密或数字签名（始终）

该策略的默认值是“已启用”。

和上一条策略的含义类似，首先系统会根据该策略判断是否进行数字加密或数字签名，如果启用该策略，系统就会知道，需要对安全通道数据进行加密或签名。然后系统会和通信的另一方进行协商，判断是否实施加密或签名。

因此，我们可以启用该策略，告诉系统我们需要进行加密或签名，然后通过上一条或下一条策略决定是否实施加密或签名。

64. 域成员：对安全通道数据进行数字签名（如果可能）

该策略的默认值是“已启用”。

有关该策略的介绍，请参考上两条策略。

签名的作用是证明数据的真实来源和数据的完整性。因为虽然可以伪造网络通信数据，但无法伪造数字证书。而且数据包一旦被篡改（哪怕一个字节的内容）数字签名就会变得无效。

65. 域成员：计算机账户密码最长使用期限

该策略的默认值是“30 天”。

该策略决定了在域环境下，计算机账户的密码在更改前可以使用的最长天数，对单机或工作组环境下的计算机无效。企业管理员可以根据实际需要以天数为单位进行指定。

66. 域成员：禁用计算机账户密码更改

该策略的默认值是“已禁用”。

该策略决定了在域环境下，域用户是否可以更改自己的计算机账户密码。如果启用该策略，那么域用户将无法修改该密码，同时上一条策略也会无效；如果禁用该策略，那么域用户可以修改自己的密码，同时必须在上一条策略设置的时间内更改自己的密码。

67. 域成员：需要强（Windows 2000 或更高版本）会话密钥

该策略的默认值是“已启用”。

该策略决定了安全数据通道进行加密或签名时所需的密钥的长度。对于 Windows NT，可以使用的密钥的长度为 56 位，这在 Windows NT 刚投入使用的时候勉强够用，因为当时的硬件性能还不是很强大，面对 56 位密钥，如果要进行破解，就需要很长的时间。然而硬件技术发展迅速，56 位密钥对于最新的处理器已经很容易破解。因此，从 Windows 2000 开始，微软为 Windows 提供了更长的密钥支持，Windows 2000 以后的系统可以支持长达 128 位的密钥。

而该策略就决定了是否使用 128 位的密钥进行加密或签名。如果网络中没有 Windows NT 系统，就可以启用该策略，增强安全性；但如果有 Windows NT 系统，为了保证和老系统的兼容性，则应该禁用该策略，继续使用 56 位密钥对安全通道进行数字加密或签名。

68. 域控制器：LDAP 服务器签名要求

该策略的默认值是空的。

该策略决定了对于 LDAP 服务器，以及客户端的通信是否要求签名。在上文我们曾介绍过 LDAP 客户端的签名要求，该策略则类似，只不过会应用到 LDAP 服务器。

需要注意的是，如果希望对 LDAP 通信进行签名，则需要将对应 LDAP 客户端和服务器的策略都设置为“需要签名”，或者将服务器端设置为“需要签名”，同时将客户端设置为“协商签名”。

69. 域控制器：拒绝计算机账户密码更改

该策略的默认值是“已禁用”。

该策略决定了是否允许域用户更改计算机账户的密码，如果希望用户可以更改计算机账户的密码，可以禁用该策略；如果希望禁止用户更改计算机账户的密码，则可以启用该策略。

70. 域控制器：允许服务器操作者计划任务

该策略的默认值是空的。

该策略决定了是否允许 Server Operators 组的成员使用 at.exe 程序提交计划任务，但该策略并不影响通过图形界面下的任务计划程序提交计划任务。

71. 账户：管理员账户状态

该策略的默认值是“已禁用”。

该策略决定了系统内建的 Administrator 账户的状态，如果希望禁用 Administrator 账户，可以将该策略设置为“已禁用”；如果希望启用 Administrator 账户，可以将该策略设置为“已启用”。该策略并不影响用户创建的其他 Administrators 组的账户。

72. 账户：来宾账户状态

该策略的默认值是“已禁用”。

该策略决定了系统内建的 Guest 账户的状态，如果希望禁用 Guest 账户，可以将该策略设置为“已禁用”；如果希望启用 Guest 账户，可以将该策略设置为“已启用”。该策略并不影响用户创建的其他 Guest 组的账户。

73. 账户：使用空白密码的本地账户只允许进行控制台登录

该策略的默认设置是“已启用”。

该策略决定了没有设置密码的账户是否可以通过网络登录，如果允许空白密码的账户网络登录，可以禁用该策略；如果禁止空白密码的账户网络登录，可以启用该策略。

如果启用该策略，那么没有设置密码的账户将只能进行控制台登录，也就是坐在本机前使用本机的键盘、鼠标和显示器登录，这种情况下，没有设置密码的用户将无法通过远程桌面登录，也不能通过网上邻居访问本机的共享文件或打印机。

74. 账户：重命名来宾账户

该策略的默认值是“Guest”。

通过该策略，我们可以将系统内建的 Guest 改为使用其他名字，这是一种安全措施。因为 Windows 中内建有 Administrator 账户和 Guest 账户，这是所有人都知道的，尤其是前者还具有系统的最高控制权。因此，任何怀有恶意的人，只要知道这台计算机运行 Windows 操作系统，那么至少知道了系统中两个有效账户的名称。如果他想入侵这台计算机，接下来只需要猜测或者破解密码即可。而只要我们把系统内建的这两个账户改名，就可以给入侵者制造一些小障碍。

75. 账户：重命名系统管理员账户

该策略的默认值是“Administrator”。

通过该策略，我们已将系统内建的 Administrator 改为使用其他的名字。关于改名的原因，请参考上一条策略。

3.3 高级安全 Windows 防火墙

目前，对计算机安全威胁最大的除了各种层出不穷的病毒和木马程序，以及间谍软件外，还有来自网络的攻击。为了防范网络攻击，最常见的办法就是安装网络防火墙。

从 Windows XP 开始，微软给 Windows 中捆绑了网络防火墙软件，该软件最初叫做 Windows 连接防火墙，自从 Windows XP SP2 开始改名为 Windows 防火墙。发展到现在，Windows 防火墙一直没有太大的改进，而该防火墙有一个最大的不足，只能对来自网络的通信进行控制，无法直接控制从本机发出的通信。

在 Windows 7 中，虽然直接从控制面板中看到的 Windows 防火墙设置界面和 Windows XP 中的相比没有太大改进，但实际上，Windows 7 中的防火墙在功能上有不小的增强，只不过这些增强的功能需要通过本地安全策略进行配置。

有关高级安全 Windows 防火墙的详细信息，我们会在本书后面的内容着重介绍，详细信息请参考 8.2 节高级安全 Windows 防火墙。

3.4 网络列表管理器策略

从 Windows Vista 开始，Windows 系统提供了一个叫做“网络位置”的功能，该功能可以将网络按照不同类型分为公用、专用和域网络三种，其中，专用网络又可细分为家庭网络和工作网络。

通过划分不同的网络类型，每当将计算机接入一个新的网络（例如需要在不同场合使用的笔记本电脑）后，Windows 防火墙就可以根据不同的网络类型，应用不同的防火墙配置文件。

例如，当将笔记本电脑使用办公室的网线连接到网络之后，即可选择“工作网络”（针对工作组环境）或“域网络”（针对域环境），随后，Windows 防火墙将使用安全设置不很严格的配置文件，例如，可能会允许文件和打印机共享，或打开某些必要的网络端口。因为这种情况，计算机接入的是我们所熟悉的且比较安全的网络，因此，此时的易用性是最重要的。

如果出门在外，将笔记本电脑使用无线网卡连接到机场提供的 WiFi 网络，此时就可以选择“公用网络”。这样 Windows 防火墙将使用安全性更高的配置文件，例如禁用网络发

现、禁用文件和打印机共享。因为这种情况，计算机接入的是我们不熟悉的，甚至可能存在危险的网络，因此，此时的安全性是首先需要保证的。

对于任何类型的网络连接，例如有线以太网、无线以太网、拨号网络、VPN 网络等，在首次连接后，都需要根据实际情况选择不同的网络位置。Windows 会记住我们的选择，下一次连接到同一个网络后，将不再需要选择，而是直接应用相应的防火墙配置文件。

网络列表管理器策略就是用于对不同网络位置下所用的防火墙配置文件进行管理的。有关这些策略，以及不同网络位置的详细介绍，请参考本书 8.3 节配置网络列表管理器策略。

3.5　公钥策略

对于一般用户，公钥策略主要是用于控制和 EFS 加密文件系统有关的密钥设置，例如，我们可以在这里管理自己的 EFS 密钥，或者设置恢复代理。有关公钥策略的作用和使用方法，请参考本书 5.4 节“EFS 加密”的内容。

> **注意**　该功能在域环境中能最大程度地发挥作用，不过在单机或工作组环境下也可以使用。因此，下文将以单机或工作组环境中一般人的典型需求为例进行简单介绍，不会做过多的深入讨论。

3.6　软件限制策略

软件限制策略是一个很好的功能，可以让我们设置允许用户运行哪些程序，不允许运行哪些程序，同时可以通过不同的规则来指定允许或者禁止运行的软件。在 Windows 的软件限制策略中，可以通过下列条件来创建规则：

- **证书规则**　通过证书规则，可以借助软件可执行程序自带的数字证书来创建策略。例如，可以通过证书规则决定所有带有来自微软的数字证书的软件都可以运行，或者所有带有某个不被信任的开发商的数字证书的软件都禁止运行。这样，每当试图运行一个程序的时候，系统都会查看该程序的数字签名，然后与软件限制策略中的定义进行比较，并根据策略的设置决定是否允许运行。
- **哈希规则**　在使用哈希规则的时候，可以指定一个软件的可执行文件，然后由操作系统计算该文件的哈希值，并根据计算出来的哈希值决定是否允许运行该软件。这样，每当试图运行一个程序的时候，系统都会计算该程序的哈希值，然后与软件限制策略中的定义进行比较，并根据策略的设置决定是否允许运行。
- **网络区域规则**　该规则主要用于使用 Windows Installer 技术安装的软件，通过该规则，我们可以对来自不同 Internet 区域的软件的安装程序采取不同的限制措施。
- **路径规则**　通过该规则，可以利用程序的安装路径或者注册表路径决定是否允许某个路径的程序的运行。

上述 4 种方式各有利弊，通常情况下，应该配合起来使用。例如，假设使用路径规则禁止运行安装在某个路径下的程序，但用户只要有相应的 NTFS 访问权限，并将软件移动到其他位置，就可以越过路径规则的限制，这时候就可以用路径规则结合 NTFS 访问权限，不允许用户移动该文件夹中的内容。有关 NTFS 访问权限的详细信息，请参考 5.2 节 NTFS 权限设置。

又如，假设通过哈希规则允许某个软件运行，但这个软件有一天升级了，升级程序对软件的主文件进行了修补，导致文件的哈希值产生了改变（要知道，对一个无论多大的文件，只要内容被改变了哪怕一个字节，该文件的哈希值也会发生巨大的变化），那么用户将无法再使用这个程序，除非管理员修改软件限制策略。这时候就可以使用证书规则来限制，毕竟无论软件怎么升级，只要开发商没有“改头换面”，该软件包含的数字证书就不会变化。

这些规则的应用还存在一个优先级问题。例如，同一个程序，如果按照证书规则来看，是允许运行的，但按照路径规则来看，是不被允许的。那么系统到底是允许还是禁止该程序运行呢？一般来说，上述四类规则按照优先级的高低排列，顺序是：哈希规则、证书规则、路径规则、网络区域规则，高优先级规则的设置会覆盖低优先级规则的设置。同时，对于同一种规则，“禁止”要优先于“允许”，例如对某个软件，我们无意中使用某种规则（例如，哈希规则）创建了禁止运行和允许运行这两条规则，那么，最终的结果是系统禁止该程序运行。

3.6.1 软件限制策略简介

运行 secpol.msc，打开本地安全策略控制台，在控制台窗口左侧的树形图中依次进入到“安全设置”→“软件限制策略”，然后在软件限制策略节点上单击鼠标右键，选择“创建软件限制策略”，这样就可以创建一个默认的软件限制策略，同时该节点下将出现名为“安全级别”和“其他规则”的两个节点（如图 3-16 所示）。下面分别介绍新出现的每个策略。

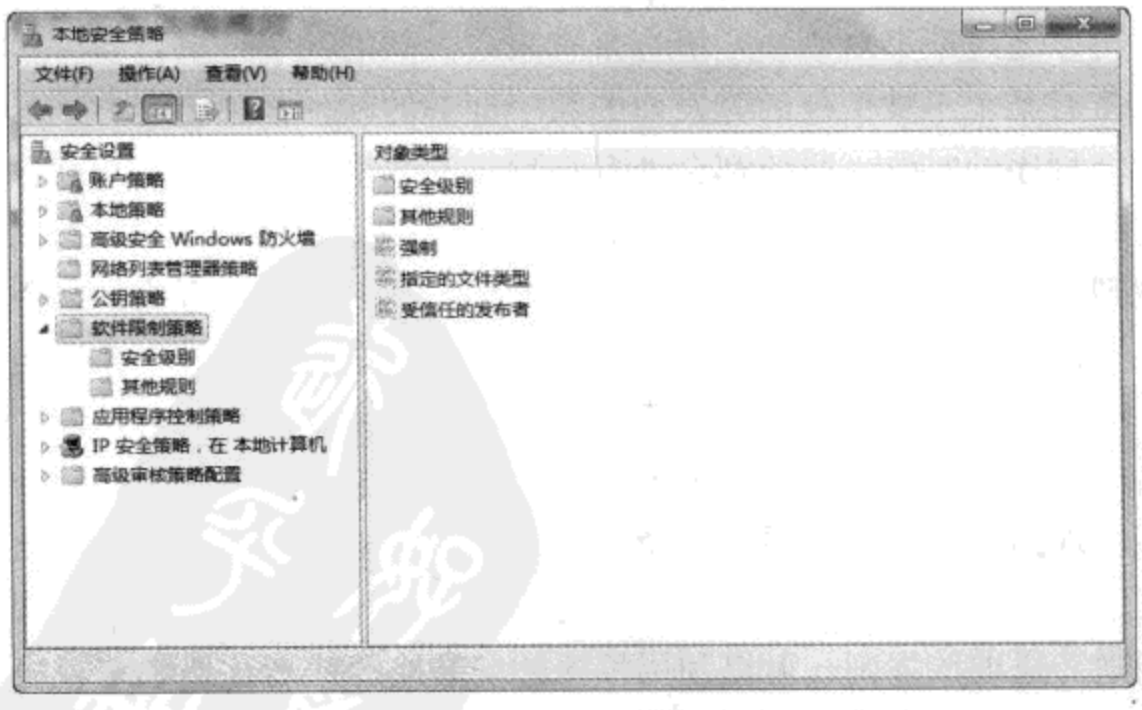


图 3-16 Windows 7 中的软件限制策略

新建了软件限制策略后，在“软件限制策略”节点下有以下三条策略。

1．强制

“强制”策略决定了软件限制策略的适用范围。单击该策略后，可以看到图 3-17 所示的对话框，在 Windows 7 中，该对话框里有三个选项：

- **应用软件限制策略到下列文件**　该选项决定了软件限制策略是否应用到库文件。简单来说，库文件为软件的运行提供支持，有时候是运行某些软件时必不可少的组件。但有时候可能有这样的情况：假设通过证书规则决定只运行某个厂商开发的软件，但该软件的运行需要的某个 DLL 文件的数字签名来自另外一个厂商，这种情况下，为了让该软件可以正常运行，就需要选择“除库文件（如 DLL）之外的所有软件文件”选项。一般情况下也建议选择该选项，毕竟大部分软件的运行都是通过一些可执行文件（例如.exe 文件）实现的，只要对可执行文件设置好限制，库文件的限制已经不再那么重要了。

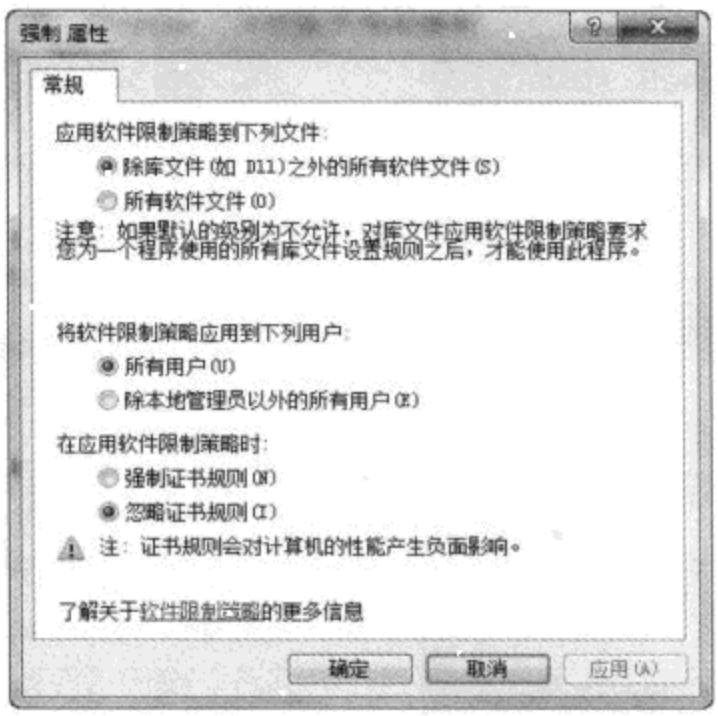


图 3-17　强制策略的设置内容

- **将软件限制策略应用到下列用户**　该选项决定了是否将软件限制策略应用于管理员用户，默认情况下，将会被应用于所有的用户。这是一种安全措施，可以让管理员被自己创建的策略所限制。在默认的设置下，如果不小心设置了错误的策略，并且可能连管理员也被禁止运行策略编辑器，或者根本无法登录，这时候可以使用 Administrator 账户登录到安全模式下修改策略。一般情况下，如果不是很必要，建议软件限制策略只对非管理员用户生效，也就是选中“除本地管理员以外的所有用户”选项。
- **在应用软件限制策略时**　该选项决定了是否在应用软件限制策略时执行证书规则。如果希望使用证书规则，请选择“执行证书规则”，如果希望禁用，请选择“忽略证

书规则”。另外，我们还可以按照 3.2.3 节安全选项中的“系统设置：将 Windows 可执行文件中的证书规则用于软件限制策略”的介绍启用证书规则。

2. 指定的文件类型

“指定文件类型”策略决定了具有什么扩展名的文件可以被视为可执行文件，如图 3-18 所示。所有由该策略指定的文件都会被系统当做可执行文件，而执行这些文件都需要经过软件限制策略的许可。如果希望添加新的文件类型为可执行文件，可以在“文件扩展名”文本框中输入目标文件类型的扩展名，然后单击“添加”按钮；如果不再希望系统将某种类型的文件当做可执行文件，可以从列表中选中目标文件类型，然后单击“删除”按钮。

3. 受信任的发布者

“受信任的发布者”策略的“属性”对话框如图 3-19 所示。默认情况下，Windows 并不允许修改这些设置，因此，首先需要选中“定义这些策略设置”选项，接下来，所有的选项都将呈可修改状态。这些选项的含义比较直观、易懂，这里不再详细介绍。

图 3-18 通过策略决定哪些类型的文件属于可执行文件

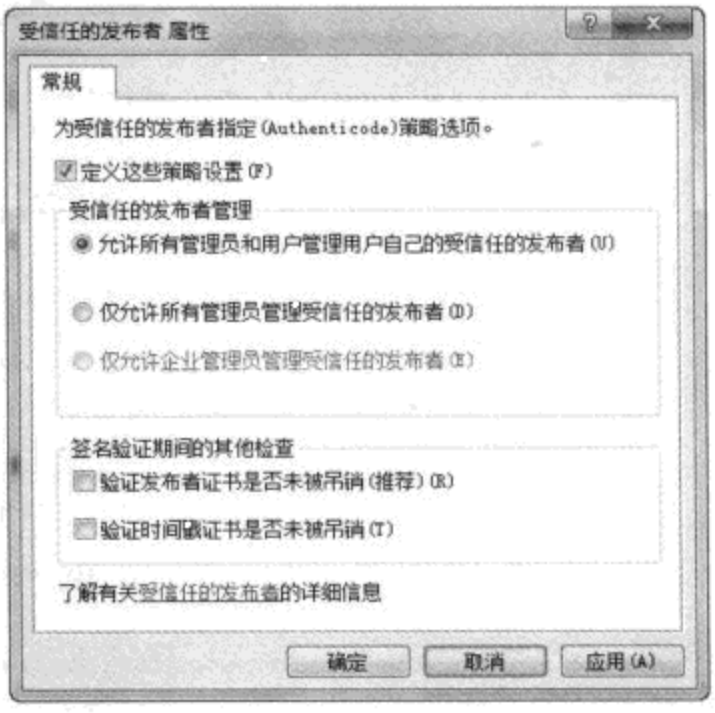


图 3-19 在 Windows 7 中设置受信任的发布者策略

进入到“安全级别”节点，Windows 7 下的该节点有三条策略：不允许的、不受限的和基本用户。这些策略都是互斥的，因此，在同一时间里，只有一条策略是生效的，也就是默认策略。默认策略的显示和非默认策略有所不同，默认策略的图标上会有一个对勾的图案。如果希望更改默认值，只需要在目标策略上单击鼠标右键，然后选择“设置为默认”即可，这样原先的默认值会被取消，系统会自动将我们新选择的策略设置为默认。

下面首先介绍“不允许的”和“不受限的”策略。“不允许的”策略的含义是：除了通过其他规则明确允许的软件外，其他软件都禁止运行；“不受限的”策略的含义是：除了通过其他策略明确拒绝的软件外，其他软件都允许运行。我们可以根据这两条策略的相应作

用，并结合自己的需要进行配置。例如，如果希望公司员工只使用特定的几个工作需要的程序，而禁止使用本机安装的其他程序，就可以将“不允许的”设为默认值，然后通过各种规则添加其他允许运行的软件；如果希望用户可以使用绝大多数软件，只禁止运行特定的几个软件，可以将“不受限的”设置为默认值，然后通过各种规则添加特定的禁止运行的软件。

除此之外，还有一个名为“基本用户”的策略，该策略的含义是：除了通过其他规则明确指定的软件外，其他所有的软件都只能以一般用户的身份运行（也就是说，不能以管理员的身份运行）。

在“其他规则”节点下，可以看到一些系统预设的规则。取决于系统的不同，以及其他策略的设置，这里可能会出现不同数量的默认规则。通常情况下，这些规则都是为了保证操作系统可以正常使用而准备的，因此，如果不是特别必要，最好不要删除或者修改这些系统自建的规则。我们可以按照需要创建自定义的规则。

在“其他规则”节点上单击鼠标右键，在出现的右键菜单中选择“新建证书规则”、“新建哈希规则”、“新建网络区域规则/新建 Internet 区域规则”或者“新建路径规则”，就可以建立对应的规则。下面来看看这些规则都是如何创建的。

3.6.1.1　证书规则

上文中已经说过，通过使用证书规则，可以通过应用程序文件的数字签名来决定是否允许运行该程序。对于这个功能，应该谨慎使用，因为--旦启用证书规则，每次运行程序的时候，系统都将对程序需要的每个可执行文件以及库文件（如果曾设置了包含库文件的话）检验数字签名，这有可能导致系统性能的降低。“新建证书规则”对话框如图 3-20 所示。

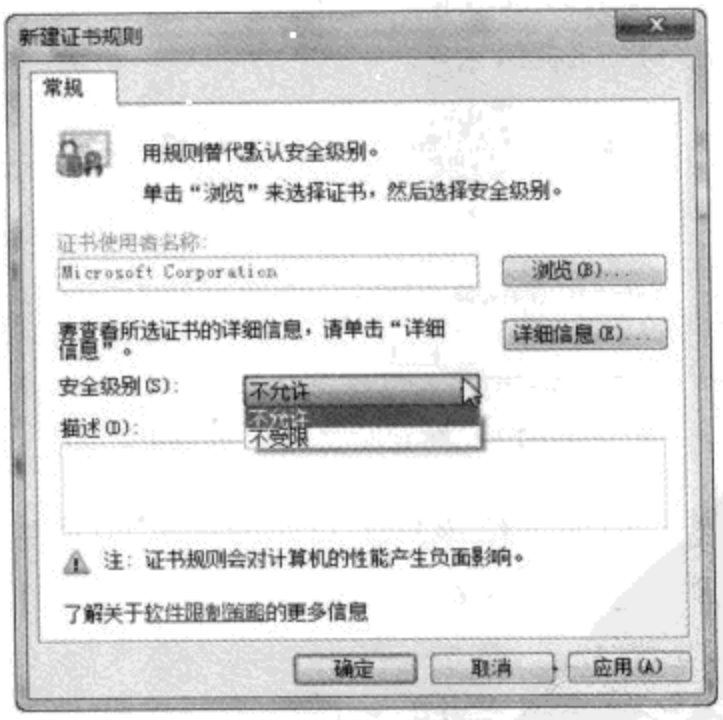


图 3-20　新建证书规则对话框

在 Windows 7 中，创建证书规则是很简单的，我们不需要专门获得软件公司的证书，

因为只要有带有数字签名的文件，Windows 7 可以自动从中提取证书。因此，可以直接单击“浏览”按钮，在随后出现的下拉菜单中定位证书。

在定位证书的时候要注意，如果已经准备好了需要添加规则的证书(.cer 或者.crt 文件)，那么，只需要在“打开”对话框中选中这些文件即可。如果手头没有需要的证书，但是想要对特定的软件进行限制，此时只要该软件带有数字签名（由正规公司新发行的软件基本上都带有)，就可以在“打开”对话框的“文件类型”下拉菜单中选择“签名的文件”选项，然后直接选择目标软件对应的主文件即可。

选择好文件或者证书后，“证书使用者名称”文本框就会变为灰色，同时显示所选证书的信息。如果需要看到证书的详细信息，可以单击右侧的“详细信息”按钮。

接下来还需要在“安全级别”下拉菜单中选择一个级别，例如是“不允许的”或者“不受限的”。

最后，为了方便日后管理众多的规则，可以在“描述”文本框中输入一定的描述性文字。

3.6.1.2 哈希规则

要创建哈希规则，请在“其他规则”节点上单击鼠标右键，选择“新建哈希规则”，随后可以看到如图 3-21 所示的对话框。

图 3-21 新建哈希规则对话框

首先，需要单击“浏览”按钮定位该规则应用到的软件的主文件，随后，系统会自动为我们指定的文件计算哈希信息，并保存到系统中，同时，在“文件信息”文本框中还会显示所选文件的详细信息。

接下来，需要根据实际需要在安全级别下拉菜单中选择不同的安全级别：不受限的、基本用户、不允许的。

最后，为了方便日后管理众多的规则，还可以在“描述”文本框中输入一定的描述性

文字。

3.6.1.3　网络区域规则

网络区域规则可以让我们针对使用 Internet Explorer 从不同区域站点下载的.msi 格式的软件安装文件的运行进行限制。要创建区域规则，请在“其他规则”节点上单击鼠标右键，选择“新建网络区域规则/Internet 区域规则”，随后可以打开“新建网络区域规则”对话框。

首先从“网络区域”下拉菜单中选择不同的网络区域，然后从“安全级别”下拉菜单选择希望进行的设置。最后，为了方便日后管理众多的规则，可以在“描述”文本框中输入一定的描述性文字。

3.6.1.4　路径规则

路径规则可以让我们对安装在某个路径下的软件，或者需要访问某个注册表路径的软件的运行进行控制。

要创建路径规则，请在“其他规则”节点上单击鼠标右键，选择“新建路径规则”，随后可以看到新建路径规则对话框。

如果要创建文件路径（可以是本地路径，例如“c:\windows”；或者 UNC 格式的网络路径，例如“\\Server\Folder”），请直接在“路径”文本框中输入路径，或者单击“浏览”按钮进行选择；如果要创建注册表路径，请直接在“路径”文本框中输入路径。在输入文件路径的时候，可以使用“*”和“?”通配符，同时还可以使用环境变量。

在给文件路径规则使用通配符的时候需要注意，如果同一个路径由不同的路径规则进行控制，那么越是具体的路径设置，可以获得的优先级就越高。例如，利用文件规则对“*.vbs”格式的文件禁止运行，但又通过文件路径规则对“\\LOGIN_SRV\Share*.VBS”设置为“不受限的”，那么这些保存在特定服务器上的.vbs 文件将可以正常运行，但在其他位置保存的.vbs 文件就无法运行。

在输入注册表路径的时候需要注意，输入的路径必须用半角的百分号（%）包起来，同时必须输入完整的根键名称，不能输入缩写。路径的格式如下：

```
%<根键名>\<键名>\<值名>%
```

例如，可以输入这样的路径：

```
%HKEY_LOCAL_MACHINE\Software\Microsoft%
```

但不能输入这样的路径：

```
%HKLM\Software\Microsoft%
```

输入好路径后，在“安全级别”下拉菜单中选择希望使用的设置。

最后，为了方便日后管理众多规则，还可以在“描述”文本框中输入一定的描述性文字。

3.6.2 软件限制策略使用建议

与软件限制策略有关的概念性内容基本上就是上面这些，如何利用这些概念创建出能够保证系统和信息安全的规则是需要长期练习的。首先，可以用 4 种不同的方式创建规则，那么，这些规则分别在什么情况下使用最合适呢？表 3-1 列出了一些常见情况下建议使用的最佳规则。

表 3-1 不同规则的适用范围

目　　的	建议使用的规则
允许或不允许运行特定版本的程序	哈希规则
允许或不允许运行始终安装在同一位置的程序	文件路径规则
允许或不允许运行可以安装在计算机上任何位置的程序	注册表路径规则
允许或不允许运行保存在中央服务器上的程序或脚本	文件路径规则
允许或不允许运行保存在中央服务器上的一批程序或脚本	带有通配符的文件路径规则
允许或不允许某个特定名称的程序运行	路径规则
允许或不允许某个特定公司开发的软件	证书规则
允许或不允许从某个 Internet 区域站点安装软件	网络区域规则

另外有一个问题需要注意，我们的设置在保证限制的同时，是否会影响到用户的使用？例如，如果需要在禁止使用其他软件的同时允许使用某个软件，那么是否只要对该软件的主程序创建一条哈希规则就可以了？这样做，该软件确实可以使用，但功能上可能会受到限制。例如，某些软件的大部分主要功能可能是借助主程序完成的，但某些功能可能需要用到其他模块，并启动额外的进程。因此，在创建规则的时候，一定要确保不仅可以保证必要软件的正常使用，还要保证所有需要的独立功能都不会受到限制。

这一方法不仅可用于解决软件限制策略中遇到的问题，而且可以解决某些应用程序的兼容性问题。例如，某些应用程序在运行中可能需要向某个特定的受保护位置写入信息，用户如果没有管理员权限，将无法正常使用这样的程序。而通过对其进行监控，了解了程序需要写入的具体位置，我们就可以针对这个位置调整权限。这样用户就算没有管理员权限，也可以对特定位置具有写入权限，很多由于权限不足而导致的应用程序兼容性问题都可以通过这种方式解决。

为了监控软件运行过程中对文件系统和注册表的读写情况，首先需要下载 Process Monitor，这是微软提供的一个免费工具，下载地址是：http://tinyurl.com/2okfn9。该软件可以实时监控系统中每个进程/线程对文件系统和注册表的访问情况。

STEP 01 为了减少监控工作的工作量，建议首先将所有其他非必要的软件全部退出，包括运行在后台的软件。然后启动 Process Monitor，并启动目标软件。

STEP 02 在该软件工具栏的最右侧有 5 个按钮，分别对应着 5 种不同类型的监控。对于本例，我们需要监控的是程序对文件系统的读写情况，因此，需要取消其他监控类型（单

击每个按钮即可开启或禁用对应类型的监控）。

STEP 03 随后，系统中所有进程的文件的读写情况都将显示在窗口中（如图 3-22 所示）。

STEP 04 虽然已经尽量关闭了其他非必要的程序，但此时系统中依然有大量进程在活动，因此，监控结果中会包含大量无关的结果。在继续操作之前，首先需要将其排除。Process Monitor 可针对进程名、访问路径等多种方式排除内容，对于本例，最简单的方法是排除进程名。因此，可以在除了目标软件的主进程之外的其他所有进程上单击鼠标右键，选择“Exclude xxx.exe”（如图 3-23 所示）。

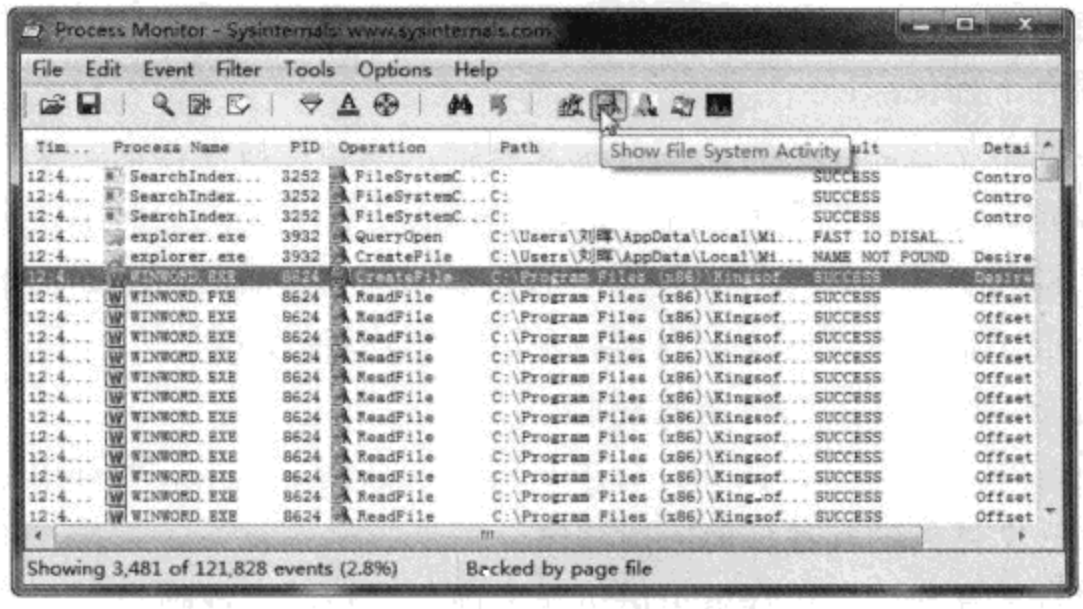


图 3-22　使用 Process Monitor 监控进程的文件读写情况

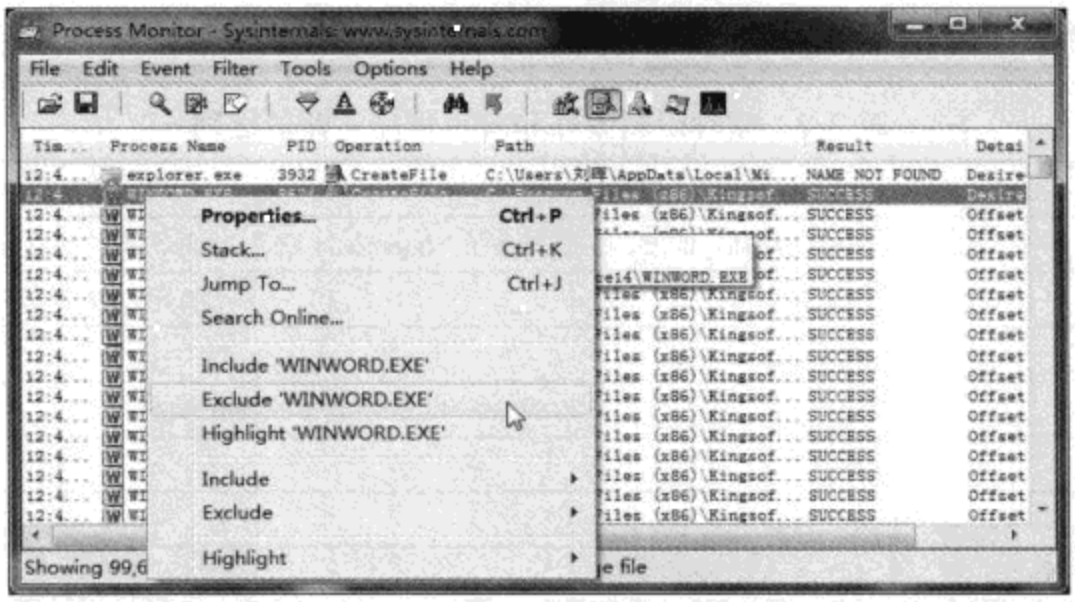


图 3-23　排除不必要的监控记录

STEP 05 经过上述操作，监控列表中只包含目标软件主程序进程的读写记录，切换到该软件的主窗口，并模仿正常使用情况下开启各项需要的功能，让 Process Monitor 监控这一过程。

STEP 06 如果一切正常，那么，在监控记录中将会新增一些进程，这些进程对应的执行文件也就是该软件运行过程中所必需的。因此，如果需要创建规则，除了对软件主程序文件创建之外，这些文件也不能忘记。

3.7 应用程序控制策略

除了软件限制策略，在 Windows 7 中还新增了一种名为 AppLocker 的应用程序控制策略。该策略与软件限制策略非常类似，但也存在一定的差别，主要是应用程序控制策略更加灵活、易用。

与从 Windows 2000 时代就存在的软件限制策略相比，Windows 7 中的应用程序控制策略（该功能只能用于 Windows 7 企业版/旗舰版，虽然专业版可用于创建规则，但无法应用这些规则）主要有下列优点：

- 可根据程序数字签名中的特定属性定义规则，例如针对发行商、文件名、文件版本等信息制定。相比软件限制策略，这种方式更加强大，因为对于带有数字签名的应用程序，即可直接允许运行多种不同的版本，就算以后的新版本也可以一个规则完全涵盖，而不需要每次程序发布新版本后都创建新的规则。
- 可针对安全组或特定的用户指派规则。
- 可为.exe 文件创建例外。例如，管理员可以通过创建规则，允许用户运行除了某个特定的.exe 文件外的其他任何应用程序。
- 规则可以导入和导出，这样就可以更简单地复制和修改规则。
- 通过使用审核模式预览在应用规则后产生的结果。

软件限制策略和应用程序控制策略的更多区别可以参考表 3-2。

表 3-2 软件限制策略和应用程序策略的区别

名　称	软件限制策略	应用程序控制策略
条件	哈希、路径、证书、注册表路径、Internet 区域	哈希、路径、发行商
规则的涵盖范围	所有用户	所有用户或指定的特定用户或组
审核模式	无	有
自动创建规则	无	有
规则的导入和导出	无	有
支持 Windows PowerShell	无	有
自定义错误信息	无	有

用一个更加形象的例子来说，对于软件限制策略，管理员可以创建类似“信任所有由某公司签名的内容”、“信任这一特定的可执行文件”或“信任位于该路径下的文件”这样的规则。但对于 Windows 7 中的应用程序控制策略，管理员可以根据应用程序的元数据，创建出类似“信任带有数字签名，并且版本号大于 12.0.0.0 的 Microsoft Office 软件”这样的规则。

综上所述，软件限制策略和应用程序控制策略各有侧重点，因此，软件限制策略现在也完全没有过时，我们需要根据实际情况，并结合两种功能的适用范围进行设置，并且在

某些要求较多的场合，可能需要同时使用这两个功能。注意，在同一个 GPO（组策略对象）中，无法同时使用软件限制策略和应用程序控制策略，如果这两类策略同时存在，Windows 7 将使用应用程序控制策略，而忽略软件限制策略。因此，如果需要同时使用，就要为这两类策略分别建立不同的 GPO。

另外需要指出的是，与软件限制策略类似，应用程序控制策略在域环境下才能发挥出最大的作用。在工作组环境下，则只能针对某台具体的计算机进行设置。不过因为有了规则的导入和导出功能，我们也完全可以在一台计算机上创建好规则并导出，然后应用于工作组中的其他计算机。这一点是软件限制策略所无法实现的。

3.7.1　规则的类型及其创建过程

运行“secpol.msc”，打开本地安全策略控制台，从左侧树形图依次进入“安全设置”→“应用程序控制策略”→“AppLocker”，随后可看到图 3-24 所示的应用程序控制设置界面。

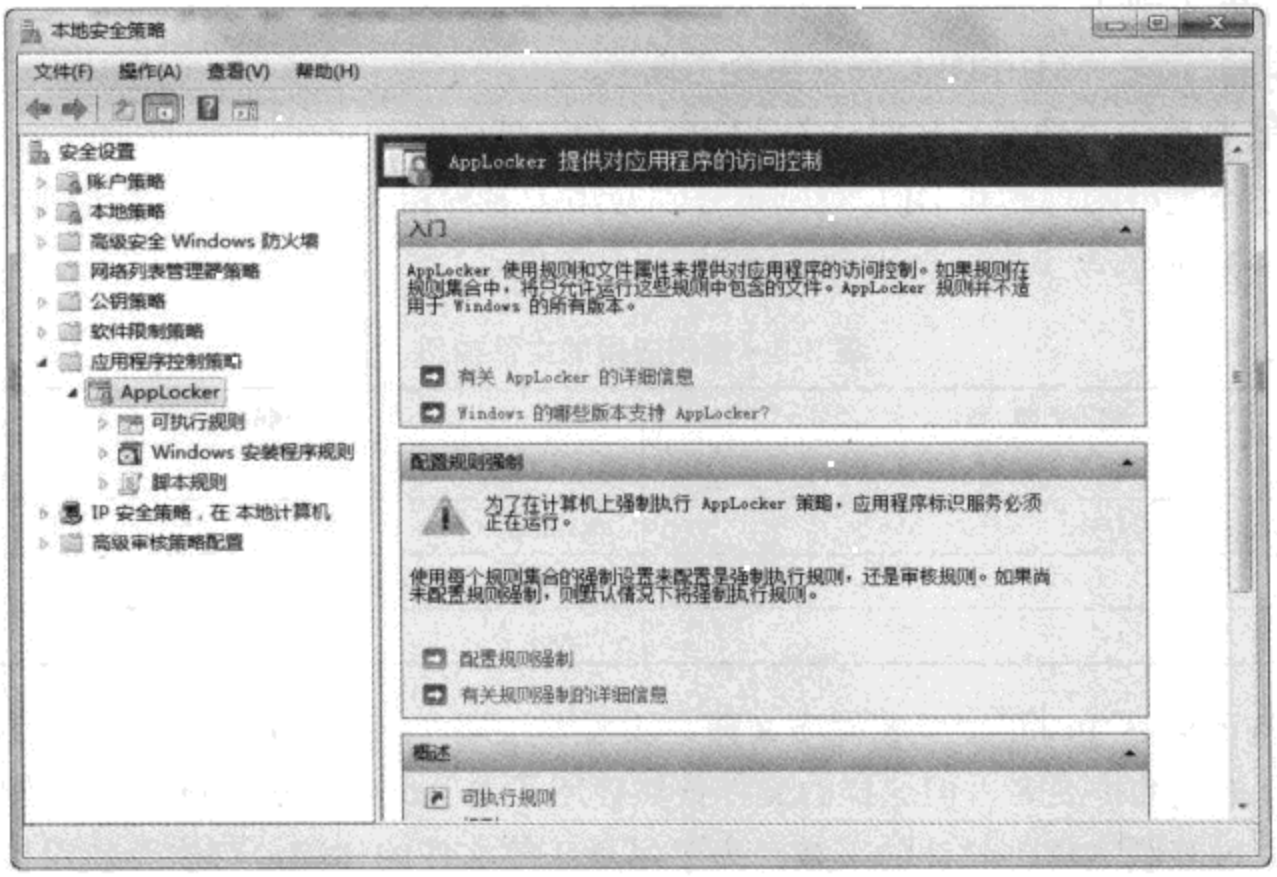


图 3-24　应用程序控制策略功能的管理界面

在 AppLocker 节点下还有三个子节点，分别对应了可设置规则的三种情况：

- **可执行规则**　该类别将影响到本机运行的所有可执行文件，以及这些程序所加载的 DLL 文件（对于 DLL 文件的限制，默认并未启用，因为启用后会对性能产生较大的影响，因此，只建议在确实需要的时候才使用）。也就是说，本机想要运行的可执行文件无论位于本地硬盘、可移动存储设备，还是网络位置，都将受到此类规则的控制。

- **Windows 安装程序规则** 该类别将影响所有使用 Windows Installer 技术的安装程序。注意，如果某软件并未采用 Windows Installer 技术，或者是根本不需要安装的“绿色软件”，那么此类软件将不受该规则的控制，这种情况可以使用“可执行规则”进行限制。
- **脚本规则** 该类别将影响本机执行的所有脚本。该规则通常适合需要使用脚本进行远程或批量管理的企业环境，小型环境下的用途通常不大。

除此之外，应用程序控制策略还可对 DLL 文件的加载进行控制。但上文已经提到过，对 DLL 文件进行控制意味着每次启动一个程序，系统必须对该程序加载的所有 DLL 文件进行检查，这样的工作将耗费大量系统资源，从而对整体性能产生非常明显的影响。因此，默认情况下，应用程序控制策略并不会对 DLL 文件生效。但如果希望控制 DLL 文件的加载，也可以按照下列步骤启用：

STEP 01 在左侧控制台树中用鼠标右键单击“AppLocker”节点，选择“属性”，打开 AppLocker 属性对话框。

STEP 02 切换到“高级”选项卡。

STEP 03 选中“启用 DLL 规则集合”选项。

STEP 04 单击“确定”按钮，关闭所有打开的对话框。

上述三个类型的规则和 DLL 规则可分别应用于多种相关扩展名的文件类型，这些类型可参考表 3-3 所述。

表 3-3 规则应用的文件类型

规 则 类 型	受影响的文件格式
可执行文件	.exe/.com
Windows Installer 安装程序	.msi/.msp
脚本	.ps1/.bat/.cmd/.vbs/.js
DLL	.dll/.ocx

对于 Windows Installer 安装程序文件，还需要注意一点，有时候我们获得的安装文件可能是.exe 格式的扩展名，但这样的文件依然使用了 Windows Installer 技术。例如，很多软件公司通过互联网提供软件的下载，为了尽量压缩文件的体积，可能会使用自解压格式对安装程序进行打包，将.msi 扩展名的文件压缩为.exe 格式。在运行这样的文件时，程序实际上会先进行“解压缩”操作，将.msi 文件释放出来，然后运行.msi 文件，并安装对应的软件。在这种情况下，此类.exe 文件的执行将先后受到可执行文件规则和 Windows Installer 安装程序规则的限制。

下面将以对已经安装的程序进行限制为例，介绍应用程序限制策略的使用方法。软件环境为 Windows 7 旗舰版，安装了各种来源的软件，但希望在确保操作系统本身可以正常运行的情况下，只允许某一特定的用户运行 Microsoft Office 软件。

STEP 01 运行“secpol.msc”，打开本地安全策略控制台，从左侧树形图依次进入“安全设置”→“应用程序控制策略”→“AppLocker”。

STEP 02 在“可执行规则”子节点上单击鼠标左键，然后单击右键，选择“创建默认规则”。

> **注意**　一定要先单击鼠标左键，再单击鼠标右键。如果是在系统启动后首次打开应用程序控制策略窗格，在修改或创建任何策略之前，一定要先左键单击对应的子节点，让控制台加载必要的组件，再右键单击，并选择要使用的功能。如果展开树形图后直接右键单击，那么，右键菜单中将只显示“帮助”命令，其他命令因为无法载入组件而无法显示。
>
> 另外要注意默认规则的创建。在应用程序控制策略中，默认规则有两个作用：确保系统内建的 Administrator 账户不受任何规则的限制，并确保在应用任何规则后，操作系统都可以正常运行。因此，在创建任何一类规则之前，都必须首先按照这里介绍的方法创建默认规则，然后根据需要创建自己的规则。默认的规则在创建好后，最好不要手工调整。如果由于调整导致 Windows 无法正常运行，甚至管理员也无法正常修改策略，则需要将计算机重新启动到安全模式下修改，重新创建默认规则。
>
> 很重要的一点是，在应用程序控制规则中，对于“禁止”规则，任何没有被规则明确允许运行的软件，都将被禁止运行。

STEP 03 再次用鼠标右键单击“可执行规则”节点，选择“自动生成规则”，打开自动生成的可执行规则向导。

> **注意**　关于自动生成规则功能
>
> 这也是相比软件限制策略更加体贴的地方。在使用应用程序控制策略时，我们可以不再完全通过自己的操作创建规则，而是可以指定要应用的应用程序，并由系统对应用程序进行分析，总结出最适合的规则。这样做不仅操作更加简便，而且可以避免由于人工操作导致的失误或错误。最重要的是，如果需要对多个软件进行限制，通过自动化的流程创建规则，可以将规则的数量降到最低，这样后期的管理就更容易。当然，如果对自动创建的规则不够满意，也可以选择“创建新规则”，然后根据需要手工创建。

STEP 04 选择该规则应用到的应用程序安装位置，以及影响到的对象。单击“浏览”按钮，选择应用程序的安装/保存位置，并单击“选择”按钮，决定该规则的使用对象（对象可以是某个用户，或某个用户组），最后还可以为该规则设置一个简单易记的名称（如图 3-25 所示）。

STEP 05 单击“下一步”按钮，随后还需要对规则进行进一步的设置（如图 3-26 所示）。在默认的设置下，对于上文所指定的目录下包含的程序文件，如果文件本身带有数字签名，

会自动创建数字证书规则；但如果文件没有包含数字签名，则可以自动创建哈希规则。绝大部分情况下，默认的设置能很好地满足要求。但如果有特殊需要，也可以根据实际情况在这里修改，例如对没有包含数字签名的文件，可以改为创建路径规则（通常不建议这样做，因为路径下的文件可能会被篡改或替换）。

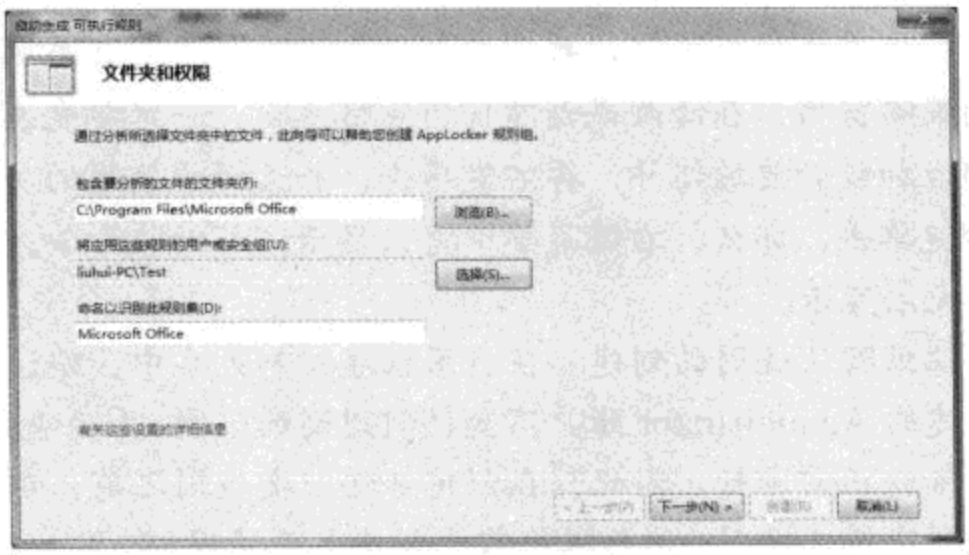


图 3-25　指定规则的应用目标和对象

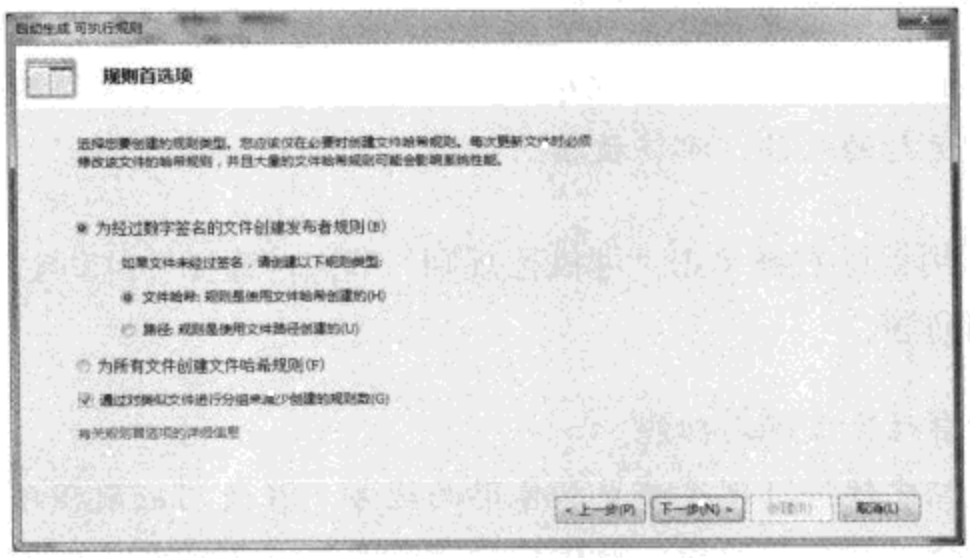


图 3-26　设定规则首选项

STEP 06　再次单击“下一步”按钮，向导会对所选目录下的所有文件进行分析，并根据上文设置的选项自动创建规则。稍等片刻后，即可看到即将创建的规则的概述（如图 3-27 所示）。例如，将要创建几条规则，这些规则的类型是什么，会影响到哪些文件。当然，通过对话框下方的链接还可以看到已经分析的具体文件是什么，以及即将创建的规则的具体内容。如果一切无误，即可单击“创建”按钮，完成创建。

STEP 07　至此，可执行规则已经创建完毕，而 Windows 安装程序规则以及脚本规则的创建步骤完全相同。不过在创建任何规则之前一定要先创建默认规则。另外，DLL 文件无法独立创建规则，因为 DLL 文件是供应用程序加载的，因此，只要对 DLL 文件启用规则，通过另外三个节点创建的所有规则都将影响到程序加载的 DLL 文件。

所有创建好的规则都将显示在控制台窗口的右侧窗格中。如果有必要，还可以对系统自动生成的文件进行修改，以便更好地满足实际需要。

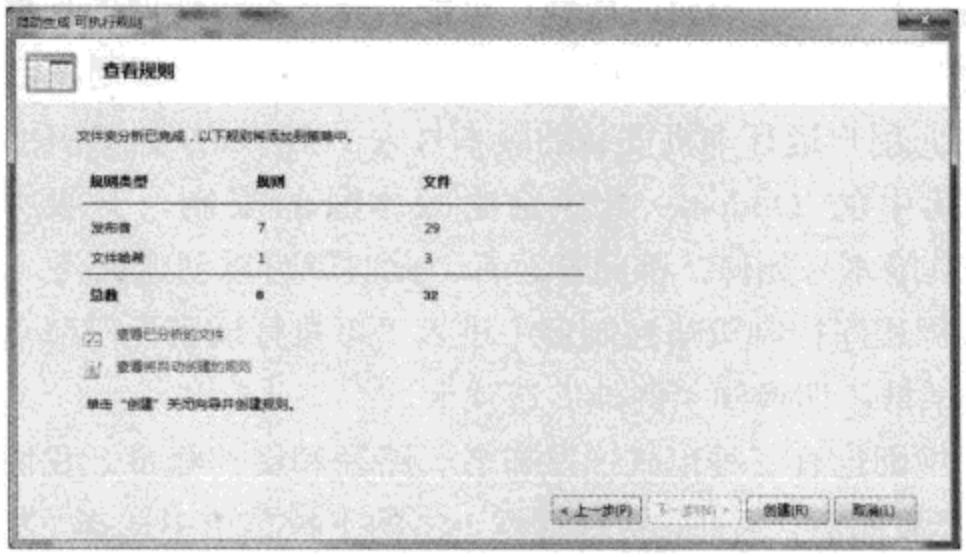


图 3-27　预览即将创建的规则

例如，对于按照上文步骤创建的执行文件规则，双击其中的一条，随后可以看到图 3-28 所示的“属性”对话框。在“常规”选项卡下可以调整这条规则的名称或描述，例如可以更改为更加简单、易懂的描述性文字，还可以选择该规则对应的是允许或者拒绝执行的操作。更重要的是，在这里可以更改该规则的应用对象。

对于证书规则，还可以通过“发布者”选项卡对发布者的相关信息进行修改（如图 3-29 所示）。例如，上文是针对 Microsoft Office 软件创建的规则，因此，“发布者”选项卡下将列出微软公司的相关信息，对于此类信息，通常没必要而且也不建议修改。不过可以根据需要调整文件的版本限制。例如，范例中使用的是 Microsoft Office 2010 产品，此时的版本号是 14.0.0.0，随后由于安装安全更新的关系，程序的版本号升级为 14.0.0.1，此时就可以借助应用程序控制策略，只允许安装过补丁程序的 Office 软件（版本选择为“14.0.0.1 及以上版本”）正常运行，未安装补丁的都无法运行。

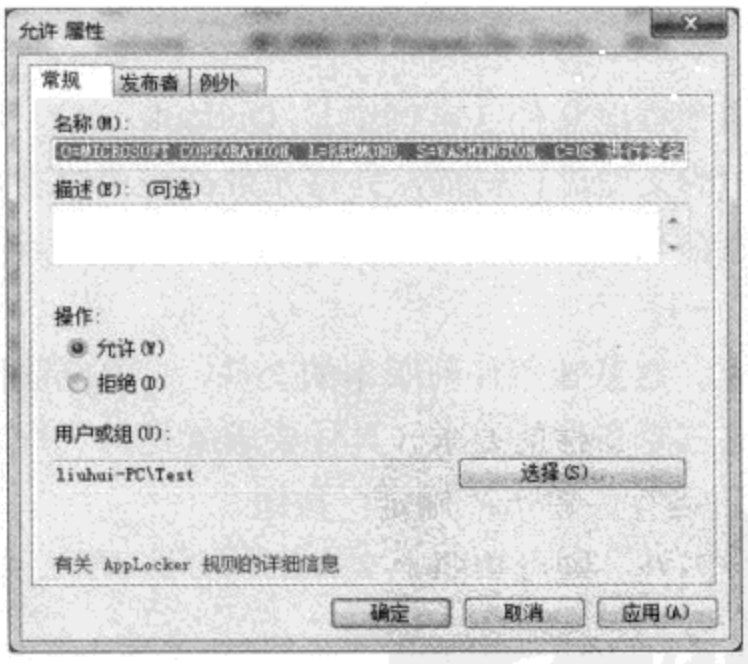


图 3-28　在这里可修改规则的属性

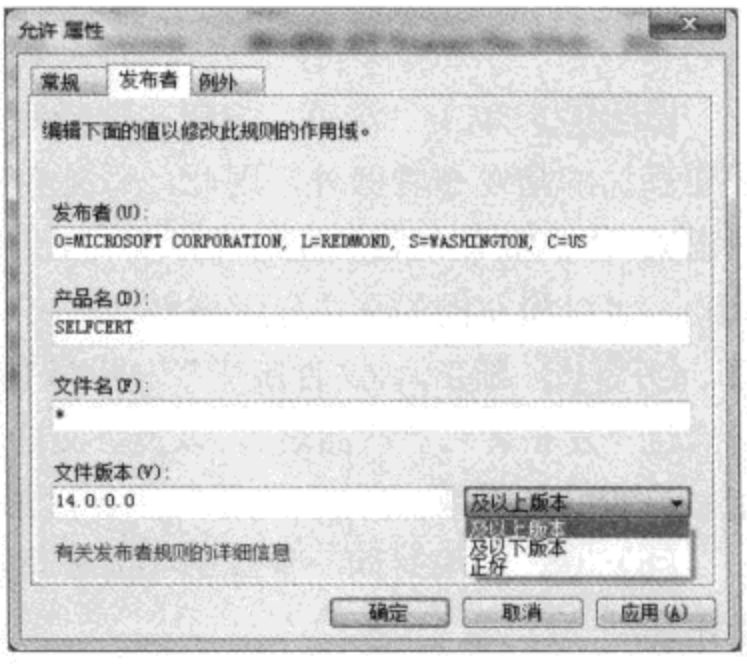


图 3-29　修改规则的发布者信息

下面重点介绍“例外”选项卡（只有证书规则可以设置例外）。有时候可能会遇到这样

的情况：对于某条已经创建好的允许规则，可能需要在某种特定的条件下实现禁止操作的目的，此时可创建例外。例如，通过按照上文介绍的方法创建规则，已经可以让 liuhui-PC 这台计算机上的 Test 用户运行本机安装的版本号大于 14.0.0.0 的 Office 软件。与此同时，我们可能希望对其中的 Outlook 组件忽略版本号的限制，只要是带有数字签名的 Outlook.exe，无论其版本号如何，都允许运行。此时就可以创建例外。

STEP 01 在应用程序控制策略控制台中进入“可执行规则”子节点，找到并双击打开目标规则的属性对话框，切换到“例外”选项卡。

STEP 02 例外规则也有三种形式：发布者、路径和文件哈希。我们可以根据实际需要进行选择，这里选择发布者，因此，从对话框上方的下拉菜单中选择“发布者”，并单击“添加”按钮，打开如图 3-30 所示的对话框。

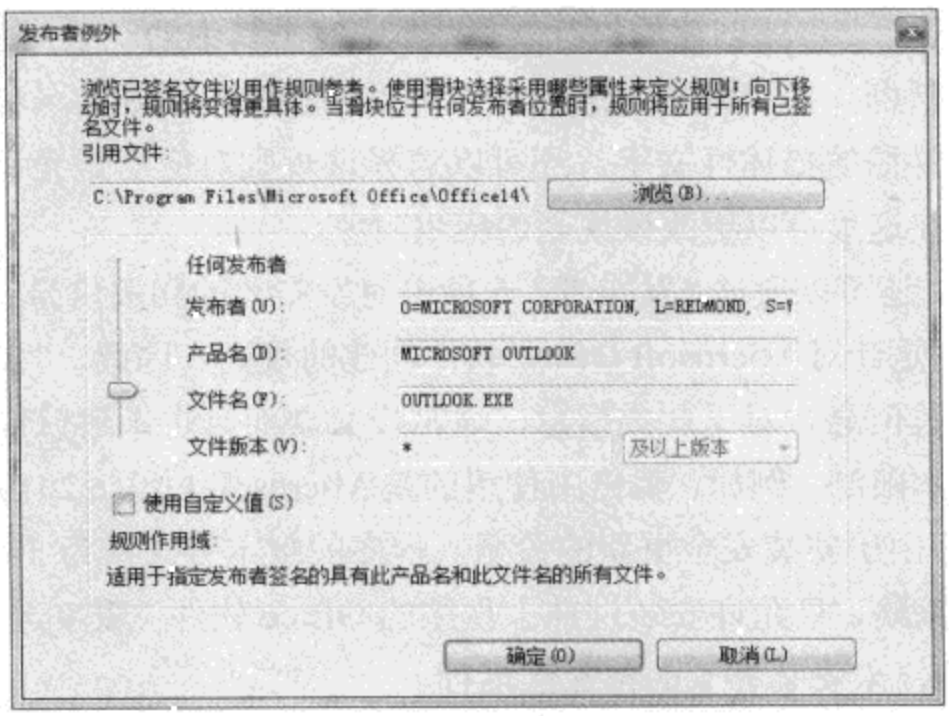


图 3-30　添加发布者例外

STEP 03 单击“浏览”按钮，选择例外应用于程序文件（本例中是 Outlook.exe）。由于要添加的是发布者例外，因此，系统会对添加的文件进行扫描，并将元数据按照级别显示出来。本例我们的目的是忽略版本号，只要带有微软数字签名的 Outlook.exe 都允许运行，因此，可以将左侧的滑块向上拖动到“文件名”一行。

STEP 04 随后，“文件版本”一栏将显示星号，这意味着任何版本的文件，只要能够**同时**满足“发布者”、“产品名”，以及“文件名”这三个条件的要求（具体要求就是每一行右侧显示的内容），则无论版本号是多少，都将允许运行。单击“确定”按钮。

STEP 05 如果对同一条规则还需要添加多个例外，则可按照上文介绍的方法重复上述操作。

从上述介绍中可以看出，应用程序控制策略要比软件限制策略简单。不过与软件限制策略类似，要想创建出完备、可靠，以及不存在疏漏的策略，一样需要反复练习和检查。因此，下文还将介绍应用程序控制策略的审核模式。

3.7.2　规则的审核

因为应用程序控制策略可以在域环境中同时应用于上千用户，因此，一旦设置存在疏漏或产生问题，可能会同时影响上千位用户。所以，在真正使用该功能的时候，首先一定要在审核模式下对该功能进行审查，只有确认一切无误之后，再真正应用。

在通过上文介绍的方法创建好所需的规则和例外后，直接用鼠标右键单击“AppLocker”节点，选择“属性”，打开图 3-31 所示的属性对话框。在“强制”选项卡下，可针对三个不同的类别分别进行设置，而可供设置的选项包括以下三个：

- **未配置**（默认设置）　等同于“强制规则”。
- **仅审核**　使用审核模式，这种情况下应用程序控制策略会生效，但并不会实际禁止某个文件的执行，只不过会将执行情况记录到事件日志中供管理员查阅。
- **强制规则**　直接应用创建的所有规则和例外，如果不符合规则和例外的要求，那么程序将无法使用。

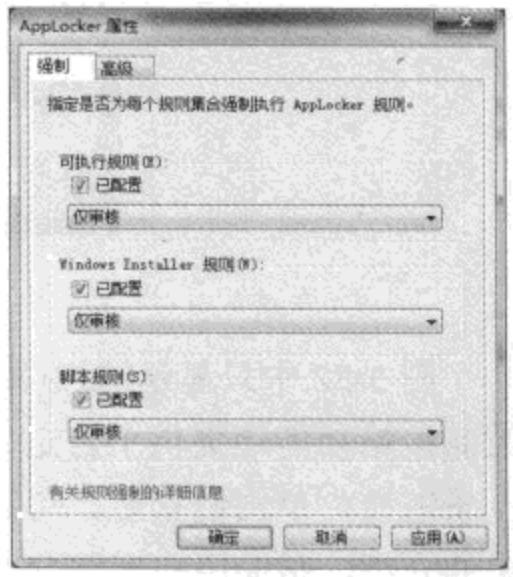


图 3-31　配置规则的应用方式

因此，只要将这三个类别都设置为“仅审核”，然后单击“确定”按钮，随后即可像正常情况一样使用计算机，并让用户照常运行自己的程序。等待一段时间后，重新使用管理员账户登录，运行“eventvwr.msc”，打开事件查看器，从左侧控制台树定位到“应用程序和服务日志-Microsoft-Windows-AppLocker”节点。在该节点下，针对不同类型的规则还可看到不同的子节点，其中包含了记录的所有事件，这些事件的相关信息见表 3-4。

表 3-4　节点包含的事件及其描述

事件 ID	事件级别	事 件 内 容	描　　述
8002	信息	【文件名】已允许运行	表示.exe 或.dll 文件被 AppLocker 规则允许
8003	警告	【文件名】已允许运行，但如果强制执行 AppLocker 策略，则可能会阻止其运行	表示如果使用强制规则，该文件将被禁止
8004	错误	【文件名】不允许运行	文件无法运行
8005	详细	【文件名】已允许运行	表示.msi 文件或脚本被 AppLocker 规则允许

通过查阅这里的规则，即可知道自己配置的策略是否满足预期目的。如果规则存在问题，还可以随时修改，并再次进行审核。在确定没问题后，可以在图 3-31 所示的对话框中将规则设置为“强制规则”，随后，该规则将针对所选的对象立刻生效。

注意　为了使强制策略或审核模式的策略正常生效，还需要启动 Application Identity

> 服务。在 Windows 7 中，该服务默认是被禁用的，因此，在配置完策略，需要审核或强制应用之前，还需要运行“Services.msc”，打开服务控制台，双击“Application Identity”服务，从启动类型下拉菜单中选择“自动”，单击“应用”按钮，然后单击“启动”按钮。
>
> 如果经过上述操作后依然无法生效，很可能是因为策略没有刷新。此时请使用管理员身份打开命令行窗口，并运行“gpupdate /force”命令刷新组策略设置。

3.7.3 自定义错误信息和规则的导入\导出

默认情况下，当用户试图执行被应用程序控制策略禁止使用的程序时，会看到类似图 3-32 所示的错误对话框。

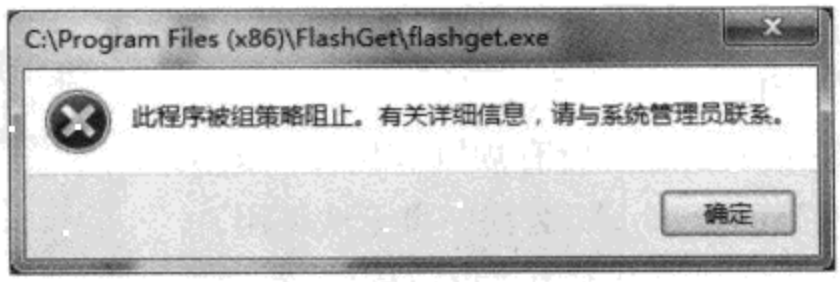


图 3-32 默认情况下的错误信息

图 3-32 中只显示这样一则信息，对于普通用户可能会造成一些困惑。因此，应用程序控制策略功能还提供了自定义错误信息的功能，该功能可以在上述错误信息对话框中添加一条链接，单击链接后，可以直接访问预定义的网页，在网页中，可以对这种限制进行简单的介绍，帮助用户理解并实施限制的意义。

要给错误信息中添加自定义的链接，可按照下列步骤操作：

STEP 01 运行“gpedit.msc”，打开组策略编辑器控制台，从左侧树形图列表中依次进入“计算机配置”→“管理模板”→“Windows 组件”→“Windows 资源管理器”节点。

STEP 02 双击“设置网页支持链接”策略。

STEP 03 选择“已启用”，并在下方的文本框中输入网页链接。这里可以输入互联网页面链接，或局域网内 Web 服务器的页面链接。

上文曾经说过，应用程序控制策略只有在域环境下才能发挥出最大的作用，例如，管理员可以针对不同的用户群体创建不同的 GPO，并设置不同的控制策略。不过在工作组环境下，类似的目标也是可以实现的。只要在一台模板计算机上配置好策略，然后导出，并导入到需要进行控制的计算机上即可。

如果需要导出策略，只需要在配置好所有的策略，并验证一切工作正常之后，在“AppLocker”节点上单击鼠标右键，选择“导入策略”，随后即可将策略导出为 XML 文件。在需要导入策略的计算机上重复上述操作，选择“导入策略”，并指定策略 XML 文件即可。

3.8　IP 安全策略

IP 安全(IPSec)策略可以在 Windows 防火墙的基础之上，对使用 IP 协议(IPv4 和 IPv6)创建的连接提供进一步的保护，例如，可对通信进行加密或添加数字签名。这些内容通常主要用于企业环境中，个人用户很少会用到。因此，本章不进行过多的讨论，在第 8 章有关 Windows 防火墙的内容中，会用一些比较实用的例子对该功能进行简单的介绍。

3.9　高级审核策略设置

在上文的介绍中曾经提到过“本地策略-审核策略”节点下可供配置的审核策略内容。通过使用这些审核策略，我们就可以知道谁在什么时间做过什么事情。上文介绍的审核策略可供审核的对象比较简单，而且审核的粒度过大，无法对审核的事件进行更进一步的细化。

不过，通过使用高级审核策略，将能对更多的内容进行审核。展开“高级审核策略配置”节点后即可看到（如图 3-33 所示），在多个子节点下分门别类地列出了各种可供审核的内容。如果希望对某个内容进行审核，只需要双击打开对应的审核策略，选择“配置以下审核事件”，并根据需要选择“成功”或“失败”即可。随后可以在事件日志中看到审核功能记录的事件。

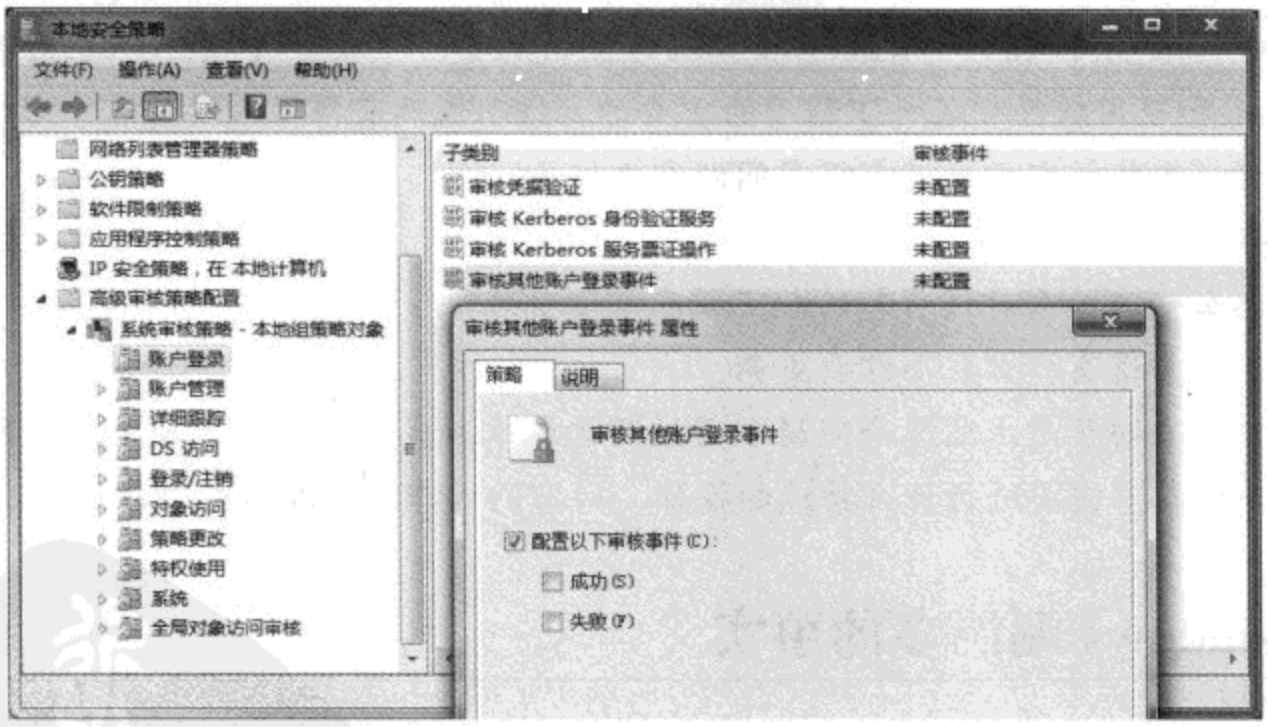


图 3-33　通过高级审核策略可对更多的内容进行审核

CHAPTER

4

第 4 章　补丁和更新

给操作系统和应用程序打补丁是保证系统安全最重要的一环，因为随着使用时间的延长，厂商可能会发现一些在测试阶段没有发现的漏洞或者问题，这时候就会发布补丁程序，对自己的程序进行修补。

在前几年，很少有人会注意更新问题。例如，2003 年初爆发的 SQL Slammer 蠕虫病毒，就是利用了微软 SQL 数据库软件中的一个漏洞广泛传播的。据分析，该蠕虫病毒在短短 10 分钟内就可以传遍全世界。顾名思义，SQL Slammer 主要是感染 SQL 数据库的，而这些数据库通常都由专人负责维护，然而该蠕虫所利用的漏洞，微软早在半年前就已经发现，并提供了补丁程序的下载，只要安装相应的补丁程序，就可以避免蠕虫的感染。遗憾的是，很多人忽视了这个问题，直接导致自己的数据受到损害，并严重加剧了整个互联网的拥堵。连专门的数据库管理人员都忽略了补丁的安装，一般用户的安全意识就更加可想而知了。

再后来，经过几次利用 Windows 漏洞传播的病毒的“教育”，很多人已经开始注意到给 Windows 和应用软件安装补丁程序的重要性。然而依然有很多人没有这个习惯，因为对很多人来说，安装补丁程序还有很多问题需要解决：

- 怎样安装补丁程序？
- 我怎么知道什么时候有新的补丁程序需要安装？
- 我怎么知道有什么程序需要更新？

本章要解决的就是上述三个问题。通过阅读本章，我们将会发现原来补丁的安装并不复杂，甚至根本不需要进行什么特殊的操作，所有的过程都会在后台自动完成。

4.1　Windows 漏洞多的事实

可能受到了很多不负责任的媒体夸大宣传的影响，很多新手认为 Windows 是一个非常不安全的操作系统，其他系统要比 Windows 更加安全。为什么会这样想？因为 Windows 经常有补丁发布，有些人可能知道，微软有一个专门的“补丁日”（每个月的第二个周二），在这一天发布大量补丁。因为补丁很多，所以漏洞很多，所以 Windows 很不安全。然而真的是这样吗？

早期的计算机用户可能还记得，当时的 Windows 3.x 甚至 DOS 操作系统的体积都很小，几张软盘就能装下。从 Windows 95 开始，Windows 的安装介质开始使用 CD-ROM 光盘，而从 Windows Vista 开始，Windows 的安装介质开始使用 DVD-ROM 光盘。所谓 Windows 的漏洞众多，其实就是这庞大的代码导致的。

因为复杂性和参与人数众多，其中任何一点微小的失误都有可能导致最终发布的软件中包含漏洞。其实这个问题不仅 Windows 会遇到，其他任何操作系统随着发展，其体积都在不可避免地增大（毕竟功能在增强），进而遇到漏洞的可能性也会不断增长。

既然如此，为什么只听到到处都在报道 Windows 的漏洞，很少有关于其他操作系统的漏洞报道？毕竟在客户端操作系统方面，Windows 的用户是最多的，全世界有无数水平高低不同的用户在使用 Windows，同时有无数质量良莠不齐的第三方程序运行在 Windows 上，另外，还有大量人员在研究和学习 Windows。可以说，Windows 所面对的威胁要比其他操作系统更加严峻。由于有广泛的“群众基础”，一旦 Windows 上遇到哪怕是微不足道的一点小问题，影响到的用户数量都将是天文数字的。

另外，我们还得考虑一个问题，那就是恶意攻击的价值。早期的计算机病毒纯粹是一种“炫技”的做法，病毒作者通过编写病毒展示自己高超的技术。然而现在的病毒已经远远脱离了这种范畴，通过编写病毒或其他恶意软件往往可以获得巨大的收益。很多人都觉得 Windows 上各种病毒层出不穷，而其他操作系统上的病毒就很少，因此，很多人觉得是 Windows 太糟糕才导致病毒太多。然而真正原因真的是这样吗？就前两年很出名的病毒“熊猫烧香”来说，这个病毒的变种很多，可以盗取用户的个人信息。那么这个病毒的作者在开发熊猫烧香的时候，是会选择全世界用户数量最多的 Windows 下手呢，还是针对其他用户数量较少的操作系统下手？结果不言而喻，既然要造成最大的影响，获得最大的收益，当然要选择用户数量最多的操作系统。目前用 Windows 的人最多，那么恶意软件制作者肯定会以 Windows 为首选目标。

上述内容主要是想让大家明白，不管什么软件，出现漏洞都是可以理解的，甚至某些情况下是不可避免的。重要的是，有了漏洞后，我们应该怎么做才能将风险降到最低。对于 Windows 以及微软发布的其他软件，自然是对其进行更新了。因为每当发现新的安全漏洞后，微软都会在最短的时间内发布相应的补丁程序，只要安装补丁程序，就能将风险拒之门外。

> **提示**　软件的更新要重视
>
> 其实任何软件都可能存在漏洞，虽然本章介绍的是微软软件的补丁，但其他软件的安全问题也不容忽视。例如，在撰写本书时，根据最新的报道，2009 年，Windows 平台上漏洞最多的程序并非 Windows 本身或微软的 Office 软件，而是 Adobe 的 Flash 和 PDF 文件（相关报道可参考：http://tinyurl.com/yj3tc6u 和 http://tinyurl.com/ycfwvmp）。因此，在确保计算机中安装的所有微软软件的状态最新的同时，其他软件的更新问题也不容忽视。

4.2 手工打补丁

对于 Windows 来说，主要的补丁有两种类型：Hotfix 和 Service Pack。通常来说，假设某个版本的 Windows 发布后遇到了安全漏洞或者其他问题，那么微软就会发布一个专门用于修复该漏洞的补丁程序。这种专门用于修复某个特定漏洞的补丁叫做 Hotfix 补丁。

然而，还有一种情况，假设某个版本的 Windows 发布很长时间了，后续发布的 Hotfix 补丁也逐渐增多，用户无论是安装还是管理这些 Hotfix 补丁，都显得比较麻烦。这时候微软往往会将以往发布的所有 Hotfix 补丁整合起来，发布一个 Service Pack 补丁。Service Pack 补丁会以数字进行编号，例如在撰写本书时，Windows Vista 已经发布过 Service Pack 1 和 Service Pack2，Windows 7 尚未公开发布任何 Service Pack。

在 Windows Vista 之前，新的 Service Pack 补丁会包含老的 Service Pack 补丁的所有内容，以及所有的 Hotfix 补丁的内容。因此，对于一个全新安装的 Windows，首先应该安装最新的 Service Pack，然后安装该 Service Pack 发布之后新发布的 Hotfix 补丁。

从 Windows Vista 开始，情况有些变化。由于采用了新的修补机制，而且由于客户端和服务器端 Windows 系统开始共用同一套 Service Pack 程序，因此，在安装新版本 Service Pack 之前，需要先安装老的 Service Pack。

听起来似乎很麻烦，不过微软已经为我们想到了很好的方法。通过微软网站，即可充分享受到 Windows 的自动更新和手动更新功能带来的便利。如果有必要，还可以在局域网中架设 WSUS 服务器，让局域网中所有的计算机通过本地服务器升级。

4.2.1 Windows Update 和 Microsoft Update

以前，微软用来给 Windows 操作系统进行更新的网站叫做 Windows Update，顾名思义，在这个网站上可以判断自己的 Windows 操作系统是否需要安装更新程序，并根据扫描结果下载和安装更新程序。

这样做有一点不足：除了 Windows，很多人的计算机上可能还安装了微软的其他软件，例如 Office、Visual Studio 等，这些程序也需要经常进行更新。因此，以前除了访问 Windows Update 网站更新 Windows 外，还需要访问其他产品的更新网站，下载这些产品的更新程序。

为了能让我们一次性将所有的微软产品的更新程序都下载和安装好，微软推出了一个叫做 Microsoft Update 的网站，通过这个网站，微软几乎所有的产品都可以得到更新。这不仅在操作上更加简单，而且因为采用了新的补丁安装技术，更新程序的下载和安装速度也更快。下面先介绍如何知道自己的系统使用的是 Windows Update 还是 Microsoft Update。

对于 Windows 7 用户，目前只能通过系统自带的更新程序进行升级，可以通过下列方法判断自己的 Windows 是使用了 Windows Update 还是 Microsoft Update。

STEP 01 在“开始”菜单中依次打开“所有程序”→“Windows Update”。

STEP 02 在随后出现的窗口（如图 4-1 所示）中查看窗口底部的“接收更新”一栏显示的内容。

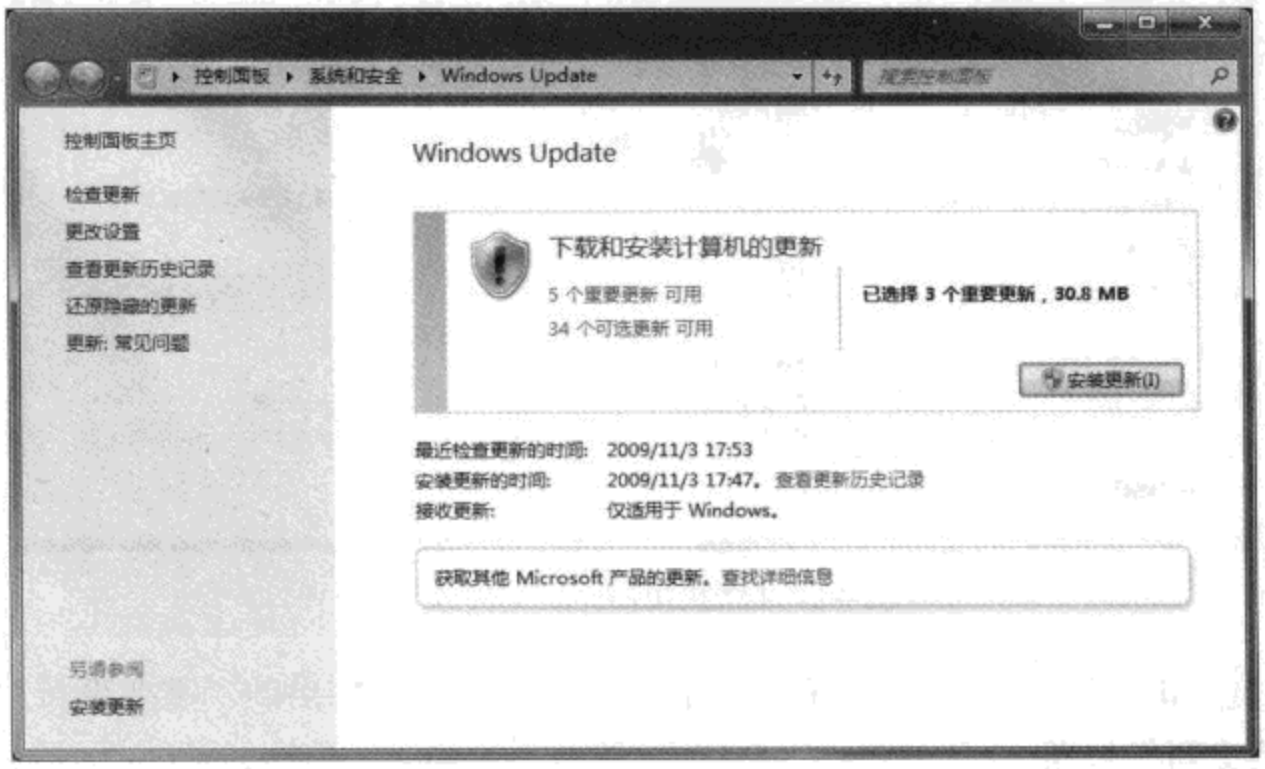


图 4-1　查看当前接收的更新类型

STEP 03 如果“接收更新”一栏显示了“适用于 Windows 产品和其他来自 Microsoft Update 的产品”的字样，表明当前系统已经在使用 Microsoft Update。

STEP 04 如果“接收更新”一栏显示了类似图 4-1 所示的“仅适用于 Windows”字样，表明当前系统依然在使用 Windows Update。

STEP 05 如果要将 Windows Update 升级为 Microsoft Update，请单击“查找详细信息”链接，并按照屏幕提示操作。

升级到最新的 Microsoft Update 站点后，即可开始给 Windows 和其他被支持的微软软件安装更新。具体的方法有两种：手工安装和自动安装。其中，手工安装比较麻烦，不过还是建议刚装好系统的时候先手工安装一次，日后可以让 Windows 自动进行更新。下文首先介绍手工安装的方法。

4.2.2　扫描和安装更新

在 Windows 7 中，更新程序的检查和安装过程非常简单，可以按照下列步骤操作：

STEP 01 打开“控制面板”，依次进入“系统和维护”→“Windows Update”（注意，尽管可能升级到了 Microsoft Update，不过这里显示的依然是 Windows Update）。

STEP 02 单击窗口左侧任务列表中的“检查更新”链接，稍等片刻，即可看到检查的结果，如图 4-2 所示。

STEP 03 取决于 Windows 的版本，以及具体的硬件配置情况，在图 4-2 中看到的内容可能会有所不同。在“下载和安装计算机的更新”类别中包含了所有重要的更新和可选更新。

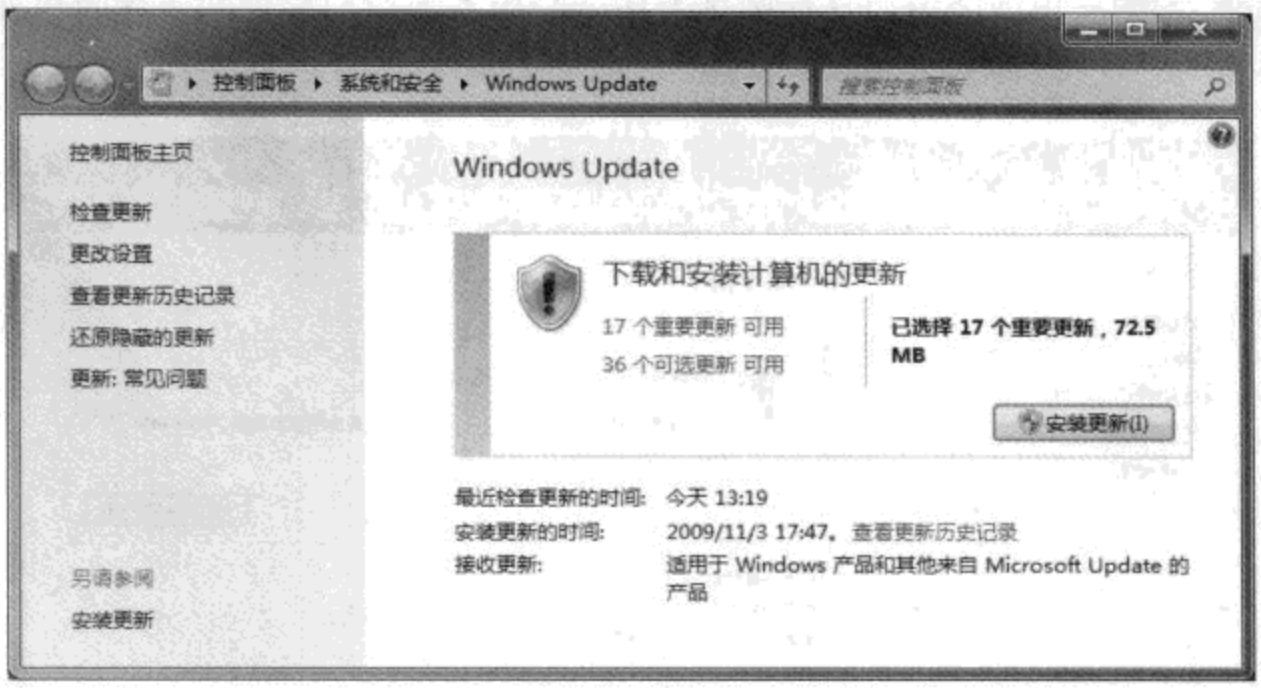


图 4-2　检测出的所有可用的更新

STEP 04　如果希望立刻安装推荐的更新（也就是图 4-2 列出的“重要更新”），可直接单击“安装更新”按钮。

STEP 05　如果希望选择要安装的更新，例如，添加某个非关键更新，或者取消安装某个关键更新，可以单击“xx 个 xx 更新可用”链接，随后可以看到图 4-3 所示的窗口。

图 4-3　选择要安装的某些更新

STEP 06　每个更新的名称前都有一个复选框，对于希望安装的更新，单击复选框将其选中；对于不希望安装的更新，则可以将其反选。选择好之后，单击“安装”按钮即可。

STEP 07　如果希望知道有关每个更新的详细信息，可以双击对应的条目，随后，Windows 会自动使用一个新的窗口显示有关该更新的信息，并提供到微软网站的链接供我们详细查看。

STEP 08　如果不希望安装某个更新，并且希望在以后检查更新的时候不再提示该更新，

可以使用鼠标右键单击该更新，选择“隐藏更新”命令。对于 Windows 7，这里还有一个改进，可以在按下“Shift”键的同时选中连续的多个更新，然后单击鼠标右键，即可批量隐藏。

STEP 09 如果希望重新提示并安装一个曾经被隐藏了的更新，只需要在图 4-2 所示的窗口中单击左侧任务列表中的“还原隐藏的更新”链接，在随后打开的页面中选中所有需要还原的更新，并单击“还原”按钮即可。

经过上述操作，在更新安装成功后，请根据需要重新启动系统，以便能够令更新生效。以后在使用 Windows 的过程中，可能会不定期出现新的更新需要安装，此时，Windows 会根据设置自动为我们下载并安装更新，并在需要的时候自动重启系统，以保证我们随时可以使用到最安全的 Windows。

4.3　自动打补丁

很多人都存在一个误区，认为打开系统的自动更新功能会让整个系统变慢，或者影响网络速度。其实这种错误的观点主要来自一些不负责任的“系统优化”技巧，因为创作这些技巧的人觉得，只要不是运行 Windows 操作系统核心功能必需的服务，就属于不重要的服务，可以放心关闭，以便加快系统的启动速度。因此，很多优化技巧建议用户关闭甚至禁用很多对系统安全密切相关的服务，例如自动更新服务。

然而，这样做的后果是什么？也许我们的系统启动速度可以快 0.1 秒，但因为无法自动安装更新，可能每周要花上好几分钟甚至十几分钟时间手工安装更新。这样对比起来，到底怎样做更合理？况且一旦因为疏忽忘记了手工更新，而恰好 Windows 中被发现了一个重大的安全漏洞，系统被借助这些漏洞传播的病毒感染了，这造成的损失又该如何挽回？

另一些人禁用自动更新的理由是自己的网络带宽有限，不希望被自动更新功能占用，其实大可不必这样担心。Windows 的自动更新功能使用了后台智能传输服务，会灵活判断当前系统的带宽使用，只有在系统空闲，并且网络也空闲的时候，才会检查和下载更新。在下载过程中，一旦系统或者网络忙碌起来，自动更新服务会立刻暂停，直到系统和网络再次空闲下来。开启了自动更新功能后，我们的正常工作根本不会受到太大影响。

4.3.1　配置和使用自动更新

对于全新安装的 Windows 7，当安装好系统且第一次登录前，设置界面上会要求配置和自动更新有关的选项。如果那时候没有配置，或者因为不了解而选择了错误的选项，那么在登录到 Windows 后，还可以按照实际需要进行调整。

> **注意**　自动更新功能只能检查和下载重要的更新。要查看、下载和安装可选更新程序，以及最新发布的驱动程序，还是需要手工进行。

在 Windows 7 中，可以按照下列步骤配置自动更新功能：

STEP 01 打开“控制面板”，依次进入“系统和维护”→“Windows Update”。

STEP 02 单击窗口左侧任务列表中的“更改设置”链接，随后可以看到如图 4-4 所示的窗口。

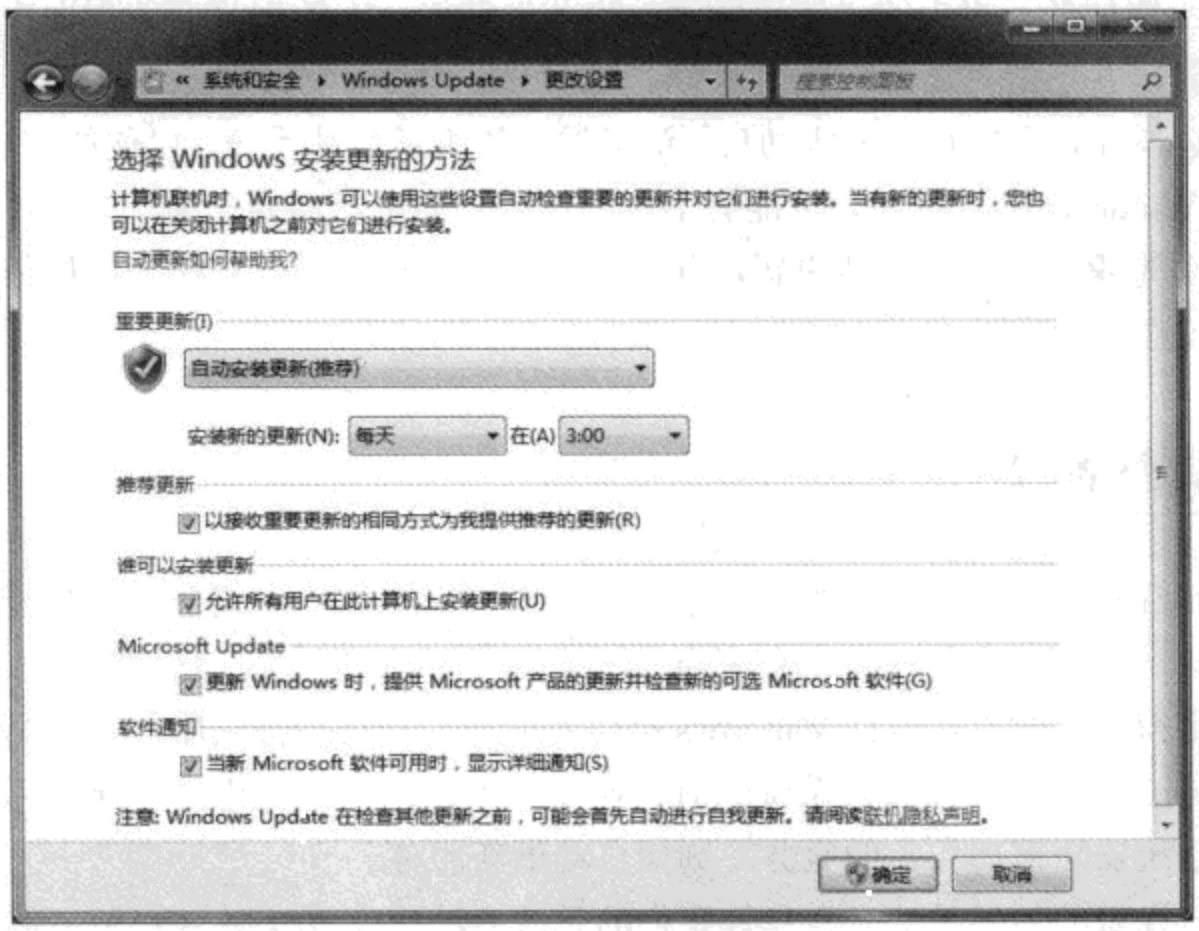


图 4-4　配置自动更新功能的工作方式

首先需要决定重要更新的处理方式，因为这类更新通常都是有关安全性或稳定性问题的补丁，因此，建议一定要第一时间安装。我们可在“重要更新”下拉菜单中选择“自动安装更新”，随后还可以通过下方的选项设置自动检查和安装的时间，例如某一天的某个时间。

如果希望自动更新功能在安装重要更新的同时，还能自动下载和安装推荐的更新，那么就可以选中“以接收重要更新的相同方式为我提供推荐的更新”选项。

在升级了 Microsoft Update 后，如果不希望再通过自动更新功能获得微软其他软件的更新，则可以取消对“更新 Windows 时，提供 Microsoft 产品的更新并检查新的可选 Microsoft 软件”选项的选择。

设置好所有的选项后，单击“确定”按钮，即可保存设置。

设置好之后，每当检测到有新的更新，系统就会根据设置自动采取对应的操作。例如，系统会开始利用空闲带宽下载，同时会在系统通知区域显示一个更新图标，将鼠标指针放在该图标上，可以看到下载进度，如图 4-5 所示。

单击系统提示区中的图标，可以打开 Windows Update 程序窗口，在这里可以查看下载

和安装的进度。更新下载完毕后，如果没有到预设的开始安装时间，Windows 7 会用一则气泡消息通知我们（如图 4-6 所示）。在看到这则消息后，如果当时正在忙碌，可以不用理会，让 Windows 等到预定的时间自动安装。如果有时间，也可以直接打开 Windows Update 窗口，并立刻安装更新。

图 4-5　自动更新功能在后台下载并等待安装

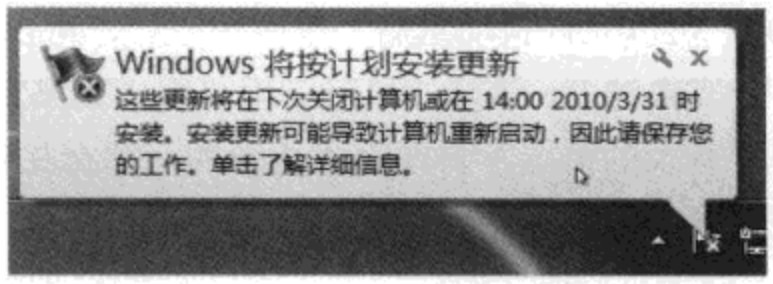


图 4-6　更新已经下载完毕，准备在计划时间内安装

4.3.2　延迟重启

Windows 的自动更新功能可以为我们自动下载和安装更新程序，但也存在一个不小的问题，那就是自动重启。我们都知道，对于很多关键更新或者安全更新，为了使更新能够成功安装，必须在安装好之后重启系统。虽然微软在 Windows 7 中采取了很多措施，尽可能地避免了绝大多数更新安装后的重启要求，但在安装少数更新后依然需要重新启动。这主要是因为更新需要替换的系统文件正在使用中，无法替换，必须重启动才能被替换完成。因此，默认情况下，当我们在 Windows 中使用自动更新功能安装了某些更新后，系统可能会用一些对话框提示我们重启系统，如图 4-7 所示。

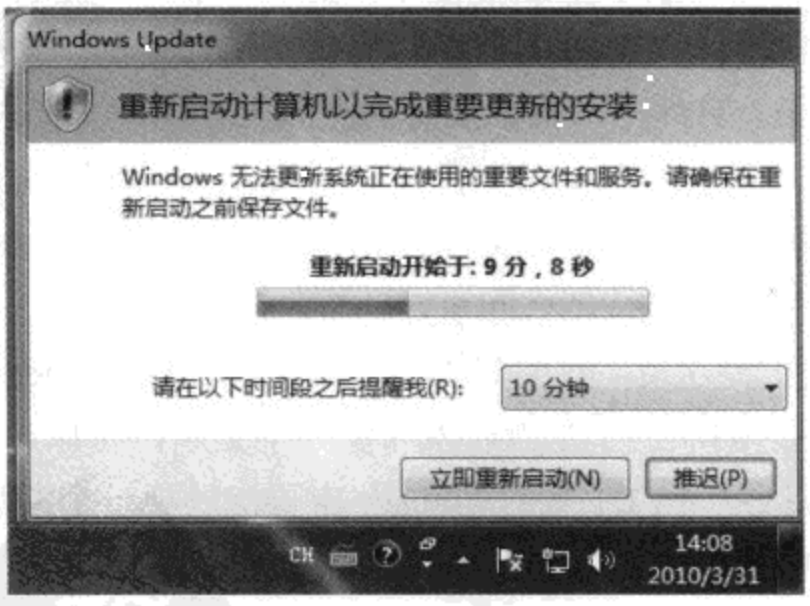


图 4-7　提示重启系统

默认情况下，系统在自动重启之前会给我们留出一定的处理时间，供我们保存当前的工作，以免造成数据丢失。如果当前有工作需要处理，不希望重启，则可以从图 4-7 所示的对话框“请在以下时间段之后提醒我”下拉菜单中选择一个提醒时间，然后单击“推迟”按钮，继续工作。

如果自动更新是在我们不在计算机前的时候完成的，而在系统留出的等待时间里我们一直没有回来，那么到时间后，系统就会自动重启，这时候没有保存的工作将会丢失。为了避免这种情况发生，可以对系统进行一些设置，运行 Regedit 打开注册表编辑器，定位到 HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU，在右侧窗格中有一个名为“NoAutoRebootWithLoggedOnUsers”的 DWORD 值，将其数值设置为“0”，可以允许自动重启，修改为“1”，可以禁止自动重启。

需要注意，该修改只对有用户登录到 Windows 的情况下有效。如果 Windows 是在没有用户登录的情况下自动完成更新的，那么在规定的时限到达后，就会立刻重新启动，不受该设置的影响。

4.4 局域网中更强大的更新

定期进行更新是一项麻烦的操作，虽然通过使用 Windows 自带的自动更新功能，不需要用户过多地干预，即可在第一时间安装最重要的安全更新，然而很多人依然希望这一过程能更加简单、快捷。尤其是某些更新程序的体积非常巨大时，其下载往往耗时长久，或者在局域网内部有多台计算机需要更新，但不希望每台计算机都反复下载相同的文件。

这些问题又该如何解决？

4.4.1 更新文件的重复使用

很多人可能还记得，在老版本 Windows 中，更新功能会将更新程序下载到本地，然后进行安装。而我们只需要将下载到本地的更新程序复制到其他计算机并执行，即可给其他计算机打补丁。对于更新，另外一个很多人所关注的内容是，以前在安装每一个更新之后，系统都会将被更新的文件备份起来，以便在确定不需要后将其卸载。为了节约硬盘空间，很多人往往会在一段时间后将这些备份文件彻底删除。然而在 Windows 7 中，根本找不到保存这些备份文件的目录，这又是怎么回事？

首先，对于更新的安装方式，我们假设这样的情况：在 Windows 发布后，发现文件 File.sys 中存在一个严重的漏洞，于是微软发布了一个更新，将原先 1.0 版本的 File.sys 文件升级为 1.1 版。一个月后，在 1.1 版的 File.sys 中再次发现一个漏洞，于是又发布一个更新，将该文件升级为 2.0 版。

如果是以前，系统必须分别下载这两个更新程序的完整文件，将 File.sys 首先升级到 1.1 版，然后升级到 2.0 版。虽然 Windows 的更新机制可以确保最终保留了最新版本的 File.sys 文件，但这种做法的弊端是很明显的：每个更新都必须下载完整的文件，浪费时间和网络流量，而且文件可能需要被更新为多个版本，并最终保留最新版本，浪费安装所需的时间。

为了解决这个问题，在新版本的 Windows 中，更新程序会更加智能地进行处理。对于上面这个例子，更新程序并不会下载每个更新的完整安装文件，而是根据情况，只下载需

要的最新版本的文件，然后替换老版本的系统文件。这样可以将要下载的文件数量减少到最低，并且可以大幅度节约安装更新程序所需的时间。

但这就导致了一个问题：每台计算机的具体配置情况都是不同的，哪怕硬件配置完全相同，也安装了相同的软件，使用时间一长，系统文件中所存在的差异将越来越大。因此，在进行更新的时候，两台计算机需要完全相同内容的概率非常低。所以，适合这台计算机的更新内容并不一定适合其他计算机，而以往将下载回来的文件直接使用到其他计算机上的做法也就完全无效了。

另外需要提及的是更新文件的备份问题。从 Windows Vista 开始，Windows 转为使用全面的模块化设计方式。对于老版本 Windows（XP 之前的系统），完全是使用 INF 文件描述的，也就是说，需要安装哪些文件，以便获得操作系统的哪些功能，这些问题都是由 INF 文件所决定的。而 Windows 7 属于模块化的操作系统，Windows 中的模块实际上就是一个或多个二进制（Binary）文件、一个编录（Catalog）文件，以及一个用于描述相关文件安装方式的 XML 文件。从相关的注册表键和服务，到文件所需要具有的安全权限等信息都包含在模块内。

在模块化的操作系统中，有一个非常重要的文件夹 WinSxS（位于 Windows 目录下），这个文件夹可以理解成包含了所有模块的一个集中的仓库。每个模块都有不同的名称，其中包含了该模块的版本、语言，以及适用的处理器架构等信息。对于操作系统，只在 WinSxS 文件夹中保存实际的模块，而我们在系统中其他位置看到的文件，以及这些文件的其他所有的实例，实际上都属于通过硬连接（Hard link）创建的到模块仓库中内容的“投影”。也就是说，在模块化的 Windows 操作系统中，每个文件的每个版本只存在一个实例，该实例位于 WinSxS 文件夹中。因此，从这个角度来看，WinSxS 文件夹实际上就代表了整个操作系统，并可等同于底层操作系统的“地基”。

在模块仓库中，并非每个模块都是正在被系统使用的，这意味着并非所有的模块都需要“投射”给操作系统。例如，对于可使用 IIS，但尚未安装该组件的系统，仓库中就存在 IIS 的相关模块，但并不会“投射”到系统中任何一个可能需要该模块的位置。

这样做有什么好处？在安装好 Windows 后，一旦需要添加某些默认没有安装的功能，就可以直接添加，而不再需要提供安装光盘；在安装更新的时候，实际上是在给仓库中添加文件的新版本，并将新版本“投射”到操作系统中其他所有需要该文件的位置，如果需要卸载某个更新，也只需要从仓库中找一个次高版本的模块进行“投射”即可，最新版本的文件依然会保留在仓库中。

鉴于此，在 Windows 7 中安装更新程序时，并不需要将老版本的文件单独进行备份，因为这些文件原本就位于模块仓库中。而也正是因为这个原因，导致 WinSxS 文件夹在刚装好系统的时候可能并不是很大，但随着使用时间的延长，会越来越大。不过要注意的是，该文件夹非常重要，不建议为了节约硬盘空间就随意删除这里的文件。

WinSxS 文件夹的体积虽然看起来很大，但实际占据的硬盘空间可能并不大。在第 3

章介绍策略安全的时候，曾介绍过一个有关硬连接的策略，并简要介绍了硬连接的创建方法。这里所说的“投射”，也正是一种硬连接的使用方式。除了 WinSxS 文件夹实际保存了系统文件外，其他位置的所有系统文件实际上都可以理解为该文件夹下内容的硬连接，这些文件虽然看起来占据了硬盘空间，但实际上都是假象。这也证明了为什么从 Windows Vista 开始，Windows 必须安装到 NTFS 分区上，除了获得更好的安全性，另一个主要原因是，只有 NTFS 文件系统的分区支持模块化“投射”所需的硬连接功能。

4.4.2 BITS 的使用和配置

Windows 7 中包含 3.5 版的后台智能传输服务（Background Intelligent Transfer Service，BITS），这是一种基于 HTTP 协议的文件传输服务，主要用于利用空闲的网络带宽传输数据时使用。这虽然也是基于标准的 HTTP 协议，但 BITS 并不会占用所有的可用带宽，甚至在没有网络连接的时候，BITS 也不会主动发起网络连接，因此，通过使用 BITS，可以在不影响其他网络工作的情况下传输容量巨大的文件（耗时可能会很长，但不会对其他工作有影响）。当然，BITS 完全可以支持“断点续传”和暂停。

在 Windows 7 中，无论是后台进行的自动更新，还是用户手工发起的更新，在下载文件时都将使用 BITS。因此，完全不用担心有限的带宽被耗光，因为 BITS 只有在网络空闲的时候才会传输数据，而且就算网络中断也没关系，下一次恢复后，BITS 还可以从断点处继续传输。

另外，在局域网中，如果通过下文介绍的策略启用对等缓存功能，还可利用 BITS 进一步加速更新程序的下载速度。在局域网中，当计算机需要使用 BITS 功能从微软服务器上下载更新文件的时候，首先会查找本地网络中其他客户端是否下载过相同的文件。如果有相同的文件，可不通过互联网，直接在本地局域网中从其他客户端处获取文件。因此，可能会令人有这样的感觉：如果局域网中包含很多 Windows Vista/7 计算机，那么第一台下载更新时需要的时间往往会长一些，但其他客户端下载时的速度好像快了很多。

其实这一切并不需要用户的干预，默认配置下就能很好地工作。不过在企业环境或其他要求较高的环境中，也可以根据实际需要，通过组策略对该功能进行更细致的设置。

要对 BITS 的行为进行配置，请运行“gpedit.msc”打开组策略编辑器，从左侧树形列表中定位到“计算机配置\管理模板\网络\后台智能传送服务（BITS）”节点，随后即可通过以下 16 条策略对 BITS 进行控制，这些策略的默认值都是“未配置”。

- **不允许 BITS 客户端使用 Windows 分支缓存** 分支缓存（Branch Cache）是 Windows 7 中的一项功能，需要配合 Windows Server 2008 R2 服务器操作系统一起使用，而该策略决定了 BITS 客户端是否允许使用 Windows 分支缓存。有关分支缓存的详细信息，可参考：http://tinyurl.com/ycfetdj。
- **不允许计算机作为 BITS 对等缓存客户端** 默认情况下，当客户端需要通过 BITS 从微软的升级服务器，或企业内部的 WSUS 服务器获得更新时，首先会尝试从距离

自己最近的对等缓存处获得文件。如果启用该策略，客户端将不再从对等缓存获得文件，而是直接从文件原始来源处下载。

- **不允许计算机作为 BITS 对等缓存服务器**　默认情况下，客户端除了可以从其他 BITS 对等缓存处获得自己所需的文件外，还可以向其他客户端提供对方所需的文件。如果启用该策略，则客户端将只能从对等缓存获得自己需要的文件，但无法向别人提供文件。
- **允许 BITS 对等缓存**　默认情况下，对等缓存功能是被关闭的，因此，在获得更新时总是必须从原始服务器获得。如果希望通过对等缓存功能加速文件的获取，以及降低中央服务器的负载，则可以启用该策略。
- **不活动BITS作业的超时**　该策略决定了当未成功完成的BITS作业在多少天没有变化时，BITS 将删除这一挂起的作业。如果未完成的作业被丢弃，BITS 会删除所有下载回来的文件。不过要注意，该策略通常并不会影响 Windows Update 下载工作，而是会影响其他需要使用 BITS 传输数据的程序。
- **限制 BITS 后台传输的最大网络带宽**　该策略可用于限制 BITS 所能使用的网络带宽，并且还可以将一天划分为两个时段（闲时和忙时），分别限制所能使用的带宽，这样可以进一步降低 BITS 对其他应用的影响。
- **限制用于对等缓存的最大网络带宽**　该策略可用于限制通过局域网用对等缓存传输数据时可用的最大带宽。默认情况下，BITS 最多只能使用 8 Mbps 的带宽，如果局域网的速度过低（例如不到 10 Mbps），则可以设置一个更小的值，以免对其他应用产生影响，但该策略并不影响 WAN 或 Internet 带宽。
- **建立一个维护计划，以限制用于 BITS 后台传输的最大网络带宽**　该策略决定了特定日期的特定时间（维护时段）里，BITS 可用的带宽数量。
- **建立一个工作计划，以限制用于 BITS 后台传输的最大网络带宽**　该策略决定了额定日期的特定时间（工作时段）里，BITS 可用的带宽数量。
- **限制 BITS 对等缓存大小**　该策略可限制本地硬盘上用于保存对等缓存内容的磁盘空间使用情况，该策略需要以百分率的形式指定最多允许对等缓存占用分区总空间的比例。
- **限制 BITS 对等缓存中文件的存在时间**　该策略决定了文件进入对等缓存后多少天后才能被删除。
- **限制 BITS 作业最长下载时间**　该策略决定了 BITS 下载工作最长可进行的时间秒数，默认值为 5400 秒，即 90 分钟。
- **限制BITS作业中允许的最大文件数**　该策略决定了一个BITS作业中最多可涉及的文件数量，通常不需要修改该设置。
- **限制此计算机的最大 BITS 作业数**　该策略决定了本机（包含所有用户、程序，以及服务）所能进行的各种 BITS 作业的最大数量。

- **限制每个用户的最大 BITS 作业数** 该策略决定了本机的每个普通用户（排除后台的服务和管理员）所能进行的各种 BITS 作业的最大数量。
- **限制可添加到 BITS 作业中的文件的最大范围数** 该策略决定了在 BITS 作业中，为作业添加的文件的范围（Range）数，也就是同一个文件可以被下载的次数。

对于小型网络环境，建议只需要启用“允许 BITS 对等缓存”策略即可，这样网络中的计算机就可以同时充当 BITS 对等缓存的客户端和服务器，并且以后在下载更新时，只要同一 IP 子网中有任何一台计算机已经下载完毕，其他需要相同文件的客户端就可以不需要从互联网上下载，而是直接从本地网络中获得，进一步加快文件的下载速度。

4.4.3 使用 WSUS 搭建内部更新服务器

对于只包含数十台电脑的小型工作组环境，微软产品的更新工作通过 Microsoft Update 网站即可很好地实现，如果该环境是由 Windows Vista/7 计算机组成的，在按照上文介绍的方法启用 BITS 对等缓存后，可以获得更好的效果。然而对于更大规模的环境，或者对于需要部署的更新希望进行严格控制的时候，还需要考虑使用其他方式。

WSUS（Windows Server Update Service）就是微软为这一环境提供的最佳解决方案。这是一个免费软件，可安装在 Windows Server 操作系统上，为局域网中的计算机提供各种微软产品的更新服务。

简单来说，该产品可实现下列目标：

- 更新的搜索和下载都在局域网内部进行，完全不需要互联网访问 WSUS 服务器可以直接从微软网站下载更新文件，或者通过可移动存储介质的方式导入更新文件。随后本地网络的所有客户端即可从内部 WSUS 服务器上检索和下载更新。而且对于包含多台 WSUS 服务器端环境，还可以指派一台或多台上游 WSUS 服务器，通过各种方式获得更新文件，其他下游 WSUS 服务器直接从上游服务器获得更新文件。
- 管理员可以对更新的发布进行审批 在客户端收到每个更新之前，管理员可以首先在测试环境中对其进行测试，一旦发现问题，例如，某个更新与企业必须使用的其他程序有冲突，则可以驳回该更新，这样客户端就可以不用安装可能导致问题的更新。
- 通过报表功能对客户端的更新安装情况进行检查 WSUS 提供了非常丰富的报表功能，可以按照多种条件对环境中更新的部署情况进行检查，例如，有多少客户端已经安装了某个特定更新，或者直接查看具体某台客户端已经安装的所有更新。
- WSUS 完全可以理解为微软 Microsoft Update 服务器的本地镜像，支持微软的各种产品的各种语种 管理员可以根据实际需要选择要包含的产品和语种，非常方便跨国公司或者多语种软件的环境。
- 可根据实际需要为客户端创建组，并在批准更新的时候将更新批准给特定的组例如，如果测试发现某个更新和 A 部门的一个软件有冲突，但和其他部门的所有软件都不

冲突，那么就可以将该更新批准给其他部门，但对 A 部门驳回。

- 对于域环境，管理员可以通过组策略将 WSUS 的配置信息推送给所有的客户端，这样客户端就可以忽略微软的更新服务器，直接从管理员指定的内部服务器上获取更新。对于工作组环境，则可以将相关的配置信息写成注册表文件（.reg），然后导入到客户端计算机中。

WSUS 需要安装在 Windows Server 2003 SP1 以上的服务器版 Windows 中，并且要求服务器安装有 IIS 和 Microsoft .Net Framework 2.0 以上版本，另外，还要求使用 SQL Server 2005 以上版本或 Windows 内部数据库。目前，WSUS 的最新版是 3.0 SP2（要为 Windows 7 提供服务，必须使用该版本或以后发布的更新版本）。有关该软件的详细介绍和下载，可访问：http://tinyurl.com/22anrz。

下文将以 Windows Server 2008 R2 作为服务器端，介绍 WSUS 的安装和配置方法。随后以 Windows 7 作为客户端，介绍通过组策略以及通过注册表文件的方式修改客户端配置的方法。其他 Windows Server 系统上的安装方式都是类似的。更详细的需求信息可参考 WSUS 的发行说明：http://tinyurl.com/ygmx22s。

4.4.3.1　WSUS 的安装和配置

1. WSUS 的安装

在一台使用默认配置全新安装的 Windows Server 2008 R2 服务器（计算机名为 WSUSServer）上，可以按照下列步骤安装 WSUS 和其他必要的组件：

STEP 01 打开服务器管理器控制台，单击窗口右侧的“添加角色”链接，打开“添加角色向导”。

STEP 02 在向导的欢迎页面上单击“下一步”按钮，并从角色列表中选中“Windows Server Update Service”。

STEP 03 随后会显示图 4-8 所示的对话框，该对话框列出了该角色所必需的其他组件。为了正确安装和使用 WSUS，这些已存组件都是必须安装的。因此，单击“添加所需的角色服务”按钮。

图 4-8　WSUS 必需的其他组件

STEP 04 单击“下一步”按钮两次，随后向导将显示可安装的角色服务。这里保持默认即可，或者也可以根据需要选中其他非必要的角色服务。选择完毕后单击“下一步”按钮两次。

STEP 05 复查摘要信息，如果一切无误，即可单击“安装”按钮开始安装。

STEP 06 在安装过程中会新出现一个配置 WSUS 安装参数的对话框（该对话框不会自动显示在前端，因此，在等待的时候需要注意任务栏是否出现了新的窗口按钮，以免浪费时间）。通常使用默认配置即可，但如果打算提供服务的产品和语种较多，那么在选择更新文件的保存位置时就要注意，一定要选择有足够硬盘空间的分区（如图 4-9 所示）。如果要针对大量的客户端提供服务，还需要考虑磁盘的访问速度，最好能选择高速硬盘或硬盘阵列。如果 Internet 访问速度不是问题，使用 WSUS 只是为了对客户端所能安装的更新进行控制，那么也可以考虑不在本地存储更新文件，此时可反选“本地存储更新”选项。这样管理员依然可以对要安装的更新进行审批，但客户端此时只需要联系 WSUS 服务器了解自己需要安装哪些更新，然后依然是通过互联网从微软的服务器上下载这些更新。

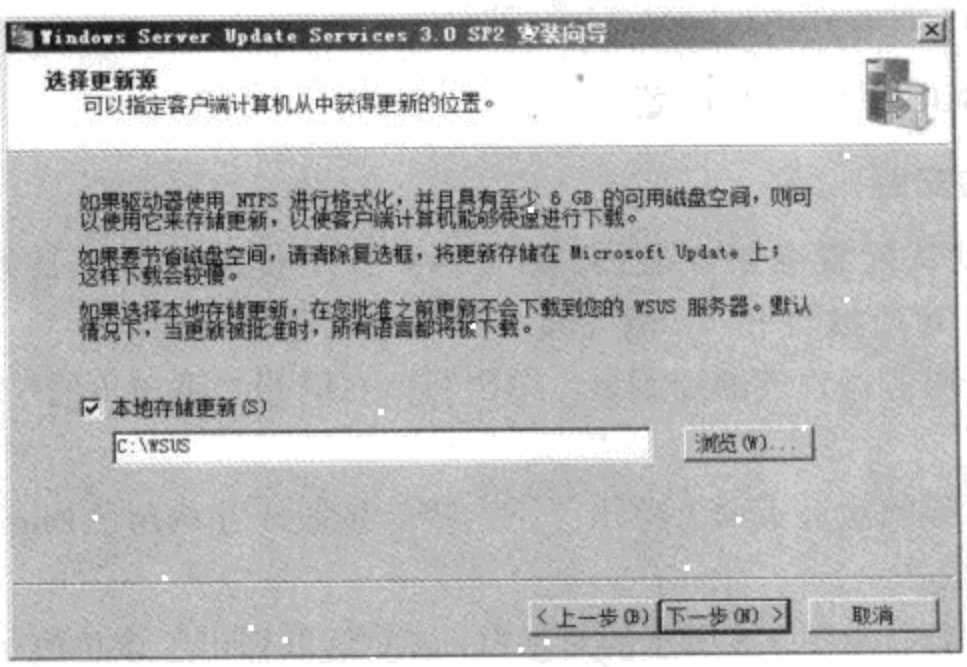


图 4-9　选择更新文件的保存位置

STEP 07 为了实现报表功能，WSUS 需要数据库的支持，因此，如果环境中已经有 SQL Server 2005 以上版本，即可直接使用这些服务器上的 SQL 实例，或者也可以安装 Windows 内部数据库（如图 4-10 所示）。Windows 内部数据库是一种简化版本的 SQL Server，主要用于保存 Windows 环境下各种软件的配置信息，不能用于其他用途。不过对于一般环境，Windows 内部数据库完全可以满足要求。

STEP 08 接着还需要对 IIS 进行配置，通常建议将 WSUS 和该功能所需的 IIS 站点安装在同一台服务器上，因此，使用默认配置即可。如果要为大量的客户端提供服务，为了改善性能，也可以使用独立的 IIS 服务器。

STEP 09 当看到“完成”按钮后，单击该按钮，完成安装工作。

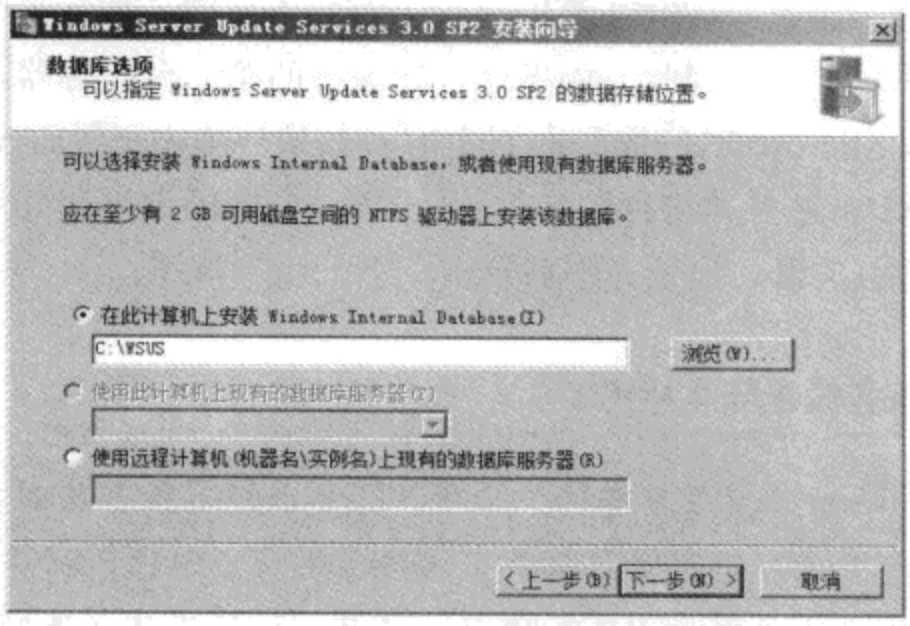


图 4-10　选择要使用的数据库实例

注意　安装文件的来源

Windows Server 2008 R2 的添加角色向导中虽然包含了 WSUS，但该程序的安装文件并未包含在 Windows 安装文件中。因此，在通过上述步骤操作时，必须确保服务器可以访问互联网，以便自动下载安装文件。如果这台服务器无法连接互联网，则可以首先从微软网站下载 WSUS 安装文件，并在服务器上运行。这样也可以安装 WSUS 以及其他所有必要的组件。

随后会看到 WSUS 的初始配置对话框，新安装的 WSUS 必须通过该对话框进行配置。但日后的管理和更新的审批工作可以使用MMC控制台在任何一台计算机上连接WSUS服务器。

2．WSUS 的配置工作

WSUS 的初始配置工作包含下列步骤：

STEP 01　在初始配置向导的欢迎页面中单击“下一步”按钮，随后可以选择是否加入 Microsoft Update 改善计划，再次单击“下一步”按钮，选择更新的同步方式，如图 4-11 所示。

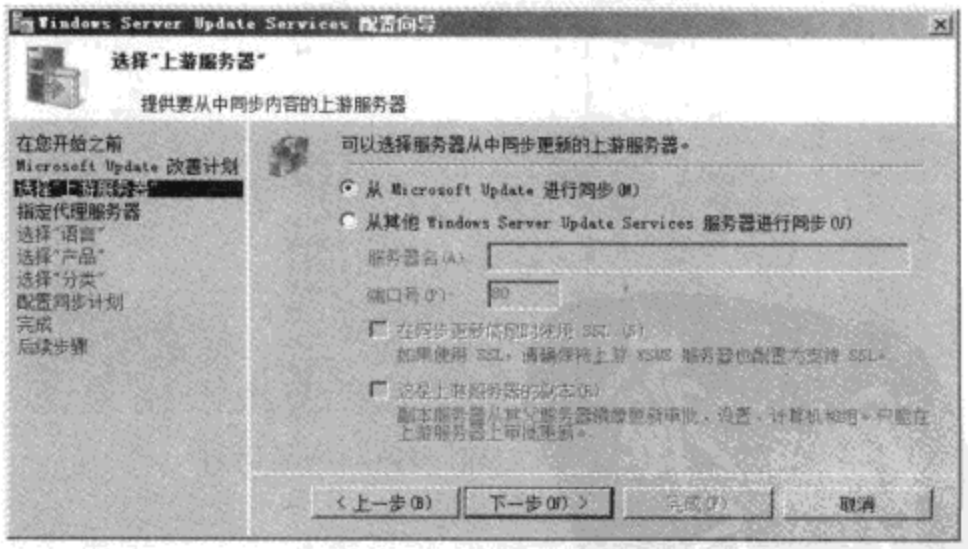


图 4-11　选择更新的获取方式

STEP 02 上文已经说过，WSUS 可以包含上游和下游服务器，其中，下游服务器可以直接从上游服务器获取更新。因此，如果这是环境中的第一台服务器，那么就只能充当上游服务器，选择“从 Microsoft Update 进行同步”；如果环境中已经有 WSUS 服务器，也可以选择“从其他 WSUS 服务器进行同步”，并设置服务器的地址和其他连接选项，此时这台服务器将充当下游服务器。设置完毕后单击“下一步”按钮。

窍门 副本服务器是什么意思？

在图 4-11 所示的对话框底部有一个选项“这是上游服务器的副本”，它将影响下游服务器的审批方式。如果不选择该选项，下游服务器可以从上游服务器获得更新，但下游服务器的管理员需要再次对更新进行审批，并应用给所有使用下游服务器的客户端。如果使用副本模式，则下游服务器将直接使用上游服务器的审批设置，也就是说，下游服务器的管理员不再需要对更新进行审批，所有上游服务器管理员批准的更新，都可通过下游服务器应用，而上游服务器管理员驳回的更新，也无法通过下游服务器安装。

STEP 03 随后可以配置代理服务器的相关参数，如果这台服务器需要通过代理服务器才能连接到互联网，即可在这里配置，否则可保留默认设置，直接单击“下一步”按钮。

STEP 04 接下来要配置可更新的产品和语种，但在此之前，服务器首先需要访问微软的更新服务器，以便获得最新的产品和语种列表。因此，需要单击“开始连接”按钮。

STEP 05 取决于互联网访问速度，等待片刻，下载完毕后单击“下一步”按钮，随后可以看到图 4-12 所示的界面。

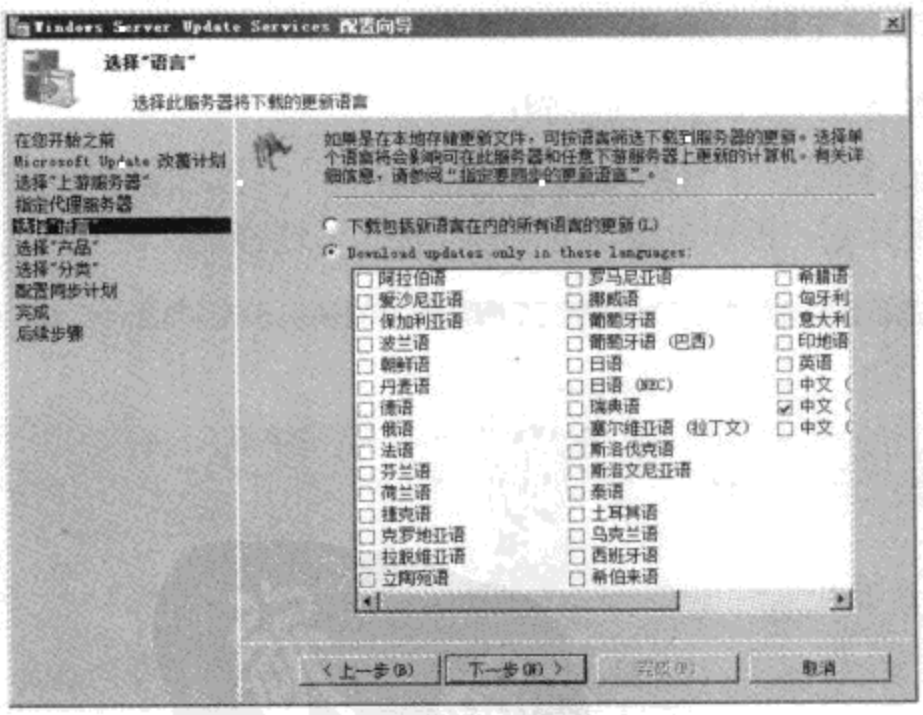


图 4-12　选择要提供服务的产品语种

STEP 06 通过 WSUS 可对微软现已支持的各种语种的产品提供更新，但通常没必要这样做，毕竟环境中可能出现的产品语种是很有限的。因此，为了减少更新文件的下载数量，

以及节省服务器占用的硬盘空间，建议只选择环境中使用的语种，然后单击“下一步”按钮。

STEP 07 随后需要选择提供服务的产品，这里列出了微软发布的所有服务。和语种的选择类似，通常没必要选择每个产品，只需要选择环境中使用的微软产品即可。选择完后单击“下一步”按钮。

STEP 08 选择可提供的更新类型（如图 4-13 所示）。在选择了所需的语种和产品后，建议选择所有类型的更新，这样客户端不仅可以获得安全更新或关键更新，还可以获得功能的补充以及驱动程序等其他所有可以通过 Microsoft Update 服务获得的内容。选择完毕后单击“下一步”按钮。

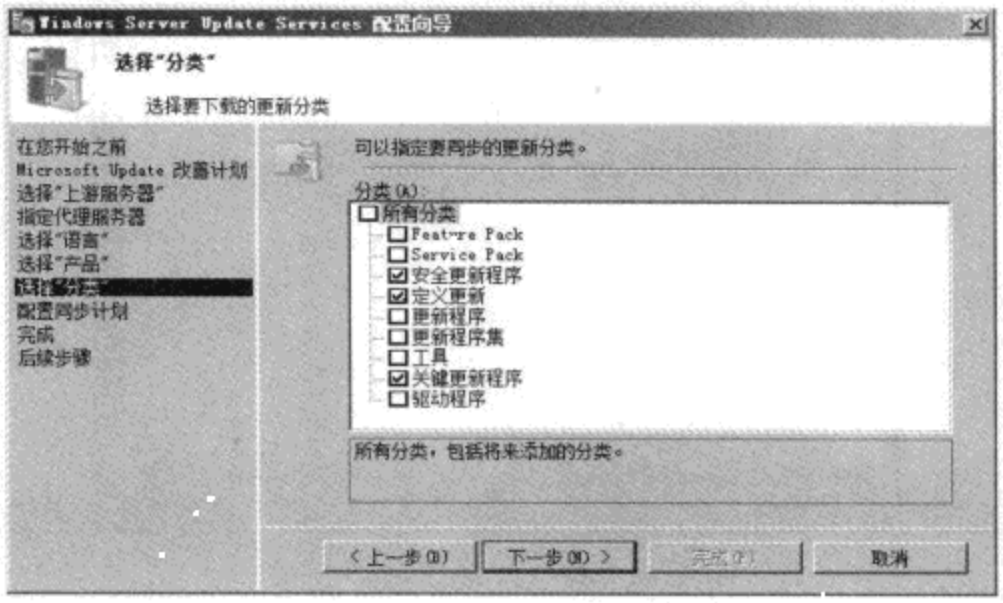


图 4-13　选择提供的更新类型

STEP 09 随后还需要设置同步方式。对于上游服务器，因为需要从微软服务器下载大量的文件，因此，第一次下载的速度将会很慢，但以后只需要下载新增的文件即可。我们可以选择自动同步，并指定同步的开始时间和频率。这里建议选择下班后的低峰时间，以免影响正常的网络工作。

STEP 10 单击“下一步”按钮，根据情况选择是否进行初始同步，并单击“完成”按钮。

如果进行初始同步，WSUS 会立刻开始进行，这个过程可能需要下载大量的文件，占据大量的网络带宽。如果希望对同步的过程进行监控，或者修改 WSUS 的其他配置，可以使用 MMC 控制台连接 WSUS 服务器，或者直接在服务器上的“管理工具”菜单中单击“Windows Server Update Service”，随后可以看到图 4-14 所示的管理界面。

WSUS 的配置涉及内容较多，限于篇幅，本章无法一一详细介绍，下面只介绍更新的审批工作。如果需要了解 WSUS 的配置方法，请参考微软网站上的相关内容，或产品自带的帮助文档。

在同步了大量更新后，WSUS 控制台首页的“待办事项”一栏会列出等待审批的不同类型的更新数量，并提供相关的链接，单击这些链接，即可对相应类别的更新进行审批。例如，在单击图 4-14 所示的安全更新的“已审批”链接后，可以看到图 4-15 所示的界面。

这里会列出当前类别下所有尚未审批的更新，鼠标右键单击一个或多个更新后，即可从右键菜单中对这些内容进行审批。如果打算批准这些更新，需要选择“审批”，随后将看到图4-16所示的界面。

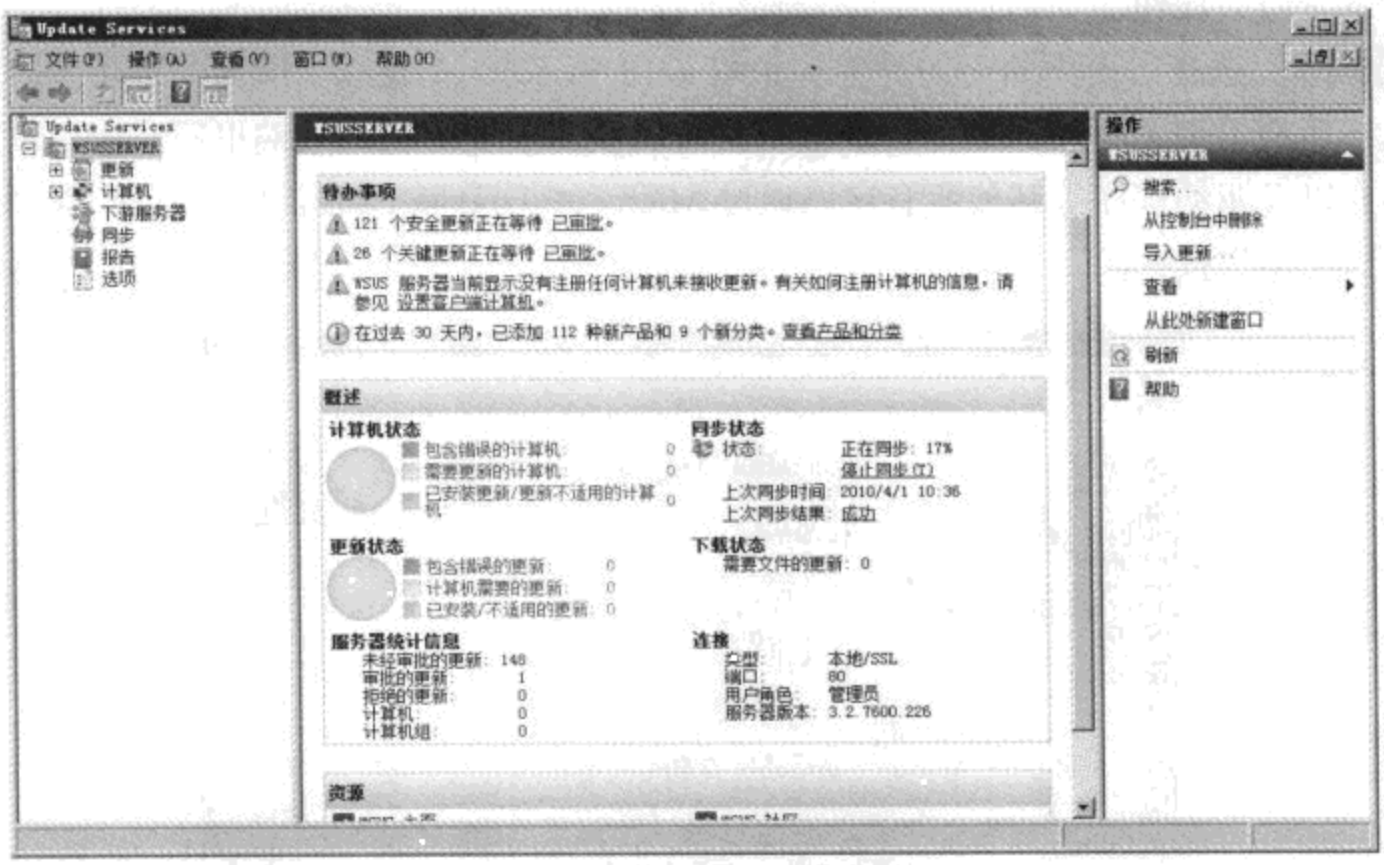


图 4-14　WSUS 的管理控制台

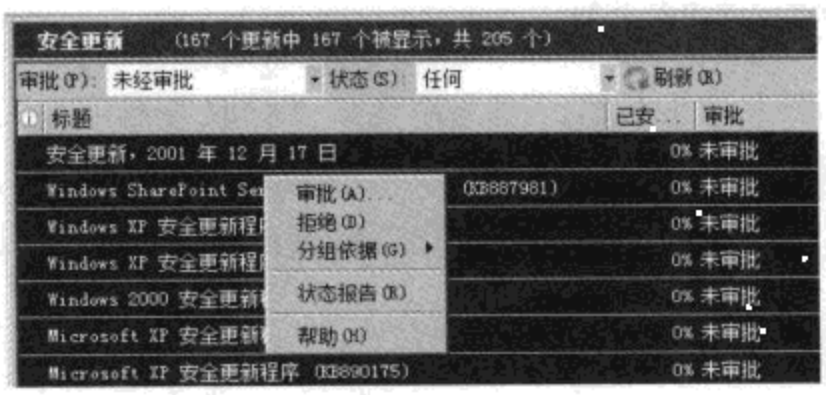


图 4-15　对更新进行批准或拒绝

图 4-16　将更新批准给不同的客户端组

上文曾经介绍过，我们可以在 WSUS 中对所有的客户端进行分组，并将更新批准给不同的组。因此，如果已经建立了客户端分组，在这里就可以分别针对不同的组决定是否批准所选的更新。如果尚未创建分组，则只有“未分配的计算机”一个选项可用。根据情况对不同的分组设置审批即可。

4.4.3.2　客户端的配置

默认情况下，客户端 Windows 系统依然会通过微软的服务器获取更新。因此，在安装并配置好内部的 WSUS 服务器后，还需要修改客户端的设置，让客户端计算机改为通过内部的 WSUS 服务器获得更新。此时有两种方法：在域环境中使用组策略，或在工作组环境

中直接应用注册表文件。

实际上，在工作组环境中也可以分别配置每台计算机的组策略，但这样需要操作，非常麻烦。因此，可以直接将配置信息编写成.reg 文件，并导入到每台客户端上。

1．通过组策略进行配置

如果需要通过组策略对客户端的更新行为进行配置，需要在域中打开相应的 GPO，并编辑 GPO 中“计算机配置\管理模板\Windows 组件\Windows Update”节点下的策略。该节点下的策略内容和含义分别如下：

- **不要在“关闭 Windows”对话框中显示“安装更新并关机”**　如果自动更新功能下载了更新，但还没有到预定的安装时间，此时关机将会直接安装更新，然后才关机。有时候这可能会需要很长时间，因此，可通过该策略决定，在遇到上述情况后，是否首先安装更新，然后才关机。
- **不要调整“关闭 Windows”对话框里的“安装更新并关机”的默认选项**　该策略决定了在使用对话框选择要执行的“关机操作”时，如果有更新已经下载，但尚未安装，是否将默认操作修改为“安装更新并关机”。
- **启用 Windows Update 电源管理以自动唤醒系统来安装计划的更新**　该策略决定了如果计算机被配置为在某个时间安装更新，但此时系统处于休眠或睡眠等节能状态，这种情况下是否将计算机唤醒，以便安装更新。
- **配置自动更新**　该策略决定了计算机是否可通过自动更新服务获得安全更新和其他关键更新，另外，还可用于配置是自动安装更新，还是在每天的特定时间安装。
- **指定 Intranet Microsoft 更新服务位置**　该策略决定了在使用内部的更新服务时，WSUS 服务器的名称或 IP 地址。
- **自动更新检测频率**　该策略决定了自动更新功能以怎样的频率向更新服务器（可以是微软的，或者内部的 WSUS 服务器）检测更新。默认情况下，该策略将使用 17～22 小时之间的一个随机值。
- **允许非管理员接收更新通知**　该策略决定了非管理员用户是否可以看到有关“有可用更新”的通知信息，并据此安装更新。
- **启用软件通知**　该策略决定了客户端计算机有可用的新软件（例如微软发布的一些用于增强 Windows 功能的免费程序）可用时，是否向计算机发出通知。
- **允许自动更新立即安装**　该策略决定了当自动更新功能获得可用的更新后，是等待到达预定时间后才安装，还是下载完之后立刻安装。
- **允许通过自动更新建议的更新**　该策略决定了计算机是否可通过自动更新功能安装非必要的建议更新，例如驱动程序。
- **对于有已登录用户的计算机，计划的自动更新安装不执行重新启动**　该策略决定了在计划的时间安装好更新，并且需要重启动才能生效时，如果计算机上已经有登录

的用户，是否重启动。建议在这种情况下不要自动重启动。

- **对计划的安装再次提示重新启动** 该策略决定了如果按照计划安装了更新，并且需要重启动，在提示用户并遭到用户拒绝后，是否再次提示用户。该策略不仅可配置是否再次提示，而且可以配置再次提示的频率。
- **对计划的安装延迟重新启动** 该策略决定了自动安装更新后，等待多久进行自动重启动。
- **重新计划自动更新计划的安装** 该策略决定了自动更新功能在系统启动完毕后，等待多长时间才开始安装已经计划好，但被漏掉的更新。如果不配置该策略，系统会自动在启动好并等待一分钟后安装漏掉的更新。
- **允许客户端目标设置** 该策略决定了该计算机所属的 WSUS 组，只有在使用 WSUS，并且在 WSUS 中建立了计算机组的情况下，才有必要使用该策略。
- **允许来自 Intranet Microsoft 更新服务位置的签名更新** 该策略决定了如果 WSUS 服务器提供的更新并非由微软签名的，而是被其他可信赖的公司签名，是否安装这样的更新。对于这条策略，目前的用途暂不明确，因为现阶段 WSUS 只能用于对微软自己的产品进行更新，无法添加其他公司的产品。根据报道，微软以后可能会通过 WSUS 以及其他软件部署技术对合作伙伴公司的软件进行更新（可参考：http://tinyurl.com/ygtclqu），因此，猜测该策略可能是针对这一计划提供的。不过在撰写本书的时候，尚无相关消息披露。

取决于具体的网络环境，配置好的策略可能需要一段时间才能应用于所有的客户端。如果希望客户端能够尽快应用，则可以在客户端上使用管理员身份打开命令行窗口，并运行“gpupdate /force”命令，强制刷新策略。如果在搭建好 WSUS 服务器后，不希望等待到预定的时间才联系服务器获得更新信息，也可以在客户端运行“wuauclt.exe /detectnow”命令，强制立刻进行检测。

2. 通过注册表文件进行配置

对于工作组环境，无法像域环境那样通过配置将变动直接应用给大量的客户端。为了简化操作，可以针对自己搭建的 WSUS 服务器，编写包含服务器相关信息的.reg 文件，然后合并到所有的客户端计算机上。但这并非最佳的解决办法，因为在注册表文件中可包含的信息并不像组策略设置那么丰富，而且依然需要有人将注册表文件手工导入到每台计算机，这依然需要大量的冗繁操作。

在工作组环境下，如果要对客户端的自动更新功能进行配置，需要使用下列注册表键：HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU

自动更新功能的配置如表 4-1 所示。

如果需要对 WSUS 环境进行配置，则需要使用下列注册表键：HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate

表 4-1　自动更新功能的配置

键　　名	值的范围和含义	数据类型
AUOptions	范围=2～5 2=下载前首先通知 3=自动下载，完成后通知 4=自动下载并按计划安装（只有存在 ScheduledInstallDay 和 ScheduledInstallTime 的值时才生效） 5=可进行自动更新，但最终用户可调整配置	32 位 DWORD 值
AutoInstallMinorUpdates	范围=0、1 0=将小型更新看做普通更新 1=静默安装小型更新	32 位 DWORD 值
DetectionFrequency	范围=*n*，其中“*n*”是指小时数（1～22） 代表两次检测周期之间的间隔时间	32 位 DWORD 值
DetectionFrequencyEnabled	范围=0、1 1=启用检测频率控制 0=禁用自定义检测频率控制（使用默认的 22 小时）	32 位 DWORD 值
NoAutoRebootWithLoggedOnUsers	范围=0、1 1=已登录用户可选择是否重启动计算机 0=自动更新功能通知用户 5 分钟后重启动	32 位 DWORD 值
NoAutoUpdate	范围=0、1 0=启用自动更新 1=禁用自动更新	32 位 DWORD 值
RebootRelaunchTimeout	范围=*n*，其中“*n*”是指分钟数（1～1440） 代表再次通知重启动之前的等待时间	32 位 DWORD 值
RebootRelaunchTimeoutEnabled	范围=0、1 1=启用 RebootRelaunchTimeout 0=禁用自定义的 RebootRelaunchTimeout（使用默认的 10 分钟）	32 位 DWORD 值
RebootWarningTimeout	范围=*n*，其中“*n*”是指分钟数（1～30） 代表在安装更新，并需要重启动时，重启动通知上显示的倒数计时时间的分钟数	32 位 DWORD 值
RebootWarningTimeoutEnabled	范围=0、1 1=启用 RebootWarningTimeout 0=禁用自定义的 RebootWarningTimeout（使用默认的 5 分钟）	32 位 DWORD 值
RescheduleWaitTime	范围=*n*，其中“*n*”是指分钟数（1～60） 代表在启动系统后，自动更新功能等待，然后才安装漏掉更新的等待时间的分钟数 该设置只影响计划的安装，并不影响最后期限。达到最后期限的更新将立刻安装	32 位 DWORD 值
RescheduleWaitTimeEnabled	范围=0、1 1=启用 RescheduleWaitTime 0=禁用 RescheduleWaitTime（下一次计划的安装时间里才尝试安装漏掉的更新）	32 位 DWORD 值

续表

键　　名	值的范围和含义	数据类型
ScheduledInstallDay	范围=0～7 0=每天 1～7=从周一到周日的特定一天 只有在 AUOptions=4 时有效	32 位 DWORD 值
ScheduledInstallTime	范围=*n*，其中“*n*”是指 24 小时格式表示的一天中的每个小时（0～23）	32 位 DWORD 值
UseWUServer	在设置该值后，WUServer 的值才会生效	32 位 DWORD 值

WSUS 环境的相关配置如表 4-2 所示。

表 4-2　WSUS 环境的相关配置

键　　名	值的范围和含义	数据类型
ElevateNonAdmins	范围=1、0 1=Users 组的用户可以接受或拒绝更新 0=只有管理员可以接受或拒绝更新	32 位 DWORD 值
TargetGroup	该计算机所属的 WSUS 计算机组的名称，要使用该设置，必须同时使用 TargetGroupEnabled	字符串值
TargetGroupEnabled	范围=1、0 1=使用客户端定向，即 WSUS 计算机组 0=不使用客户端定向，要使用该设置，必须同时使用 TargetGroup	32 位 DWORD 值
WUServer	用于获得更新的 WSUS 服务器的 URL，要使用该设置，必须同时使用 WUStatusServer，并且这两个值设置的内容必须相同	字符串值
WUStatusServer	用于将客户端安装信息发送到的统计报表服务器的 URL，要使用该设置，必须同时使用 WUServer，并且这两个值设置的内容必须相同	字符串值

在知道需要调整的注册表值的具体内容后，还需要了解如何编辑出符合自己要求的.reg 文件。限于篇幅，这里不准备详细介绍，感兴趣的读者可参考微软知识库中的文章：http://tinyurl.com/6o8wb。

下面列举一个例子，通过将这些内容粘贴到记事本中，然后保存成“.reg”文件，随后将文件复制到其他计算机，双击即可导入，并应用所需的设置。如果不确定怎样编写正确的.reg 文件，也可以在一台计算机上按照上文的介绍手工修改注册表键，然后将修改的内容导出成.reg 文件，并应用给其他计算机。

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]
"RescheduleWaitTime"=dword:00000002
"NoAutoRebootWithLoggedOnUsers"=dword:00000001
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000003
"ScheduledInstallDay"=dword:00000000
```

```
"ScheduledInstallTime"=dword:0000000C
"UseWUServer"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
"WUServer"="http://WSUSServer"
"WUStatusServer"="http://WSUSServer"
```

4.5　使用 MBSA 执行安全性扫描

通过使用上文介绍的方法，我们可以为整个环境中的所有计算机安装更新。那么除了使用 WSUS 的报表功能，如何知道每台计算机是否缺少哪个更新，或者是否有其他安全问题？此时可以使用微软免费提供的 MBSA（Microsoft Baseline Security Analyzer，微软基准安全分析器）工具，对本机或者网络上的计算机进行扫描，找出可能存在的漏洞或安全弱点。

该工具的详细介绍和下载地址可访问：http://tinyurl.com/yzw2sd9。

该工具可扫描目标计算机上所有可被 Microsoft Update 支持的产品是否安装了安全更新或关键更新，并且还可以扫描常用微软产品的配置是否存在安全隐患。该工具不仅提供了 GUI 版本可供扫描本机或多台网络计算机，而且可在命令行下使用，还可以通过脚本直接调用，实现更多强大的功能。

下面将介绍如何使用该工具的 GUI 版本对本机以及网络上的其他计算机执行安全检测：

STEP 01 确保进行扫描的计算机可以连接到互联网或内部的 WSUS 服务器，然后启动 MBSA 工具。

STEP 02 在程序的欢迎页面中，需要选择扫描的计算机数量（一台或多台），本例将扫描多台，因此，直接单击“Scan multiple computers”，随后可以看到图 4-17 所示的界面。

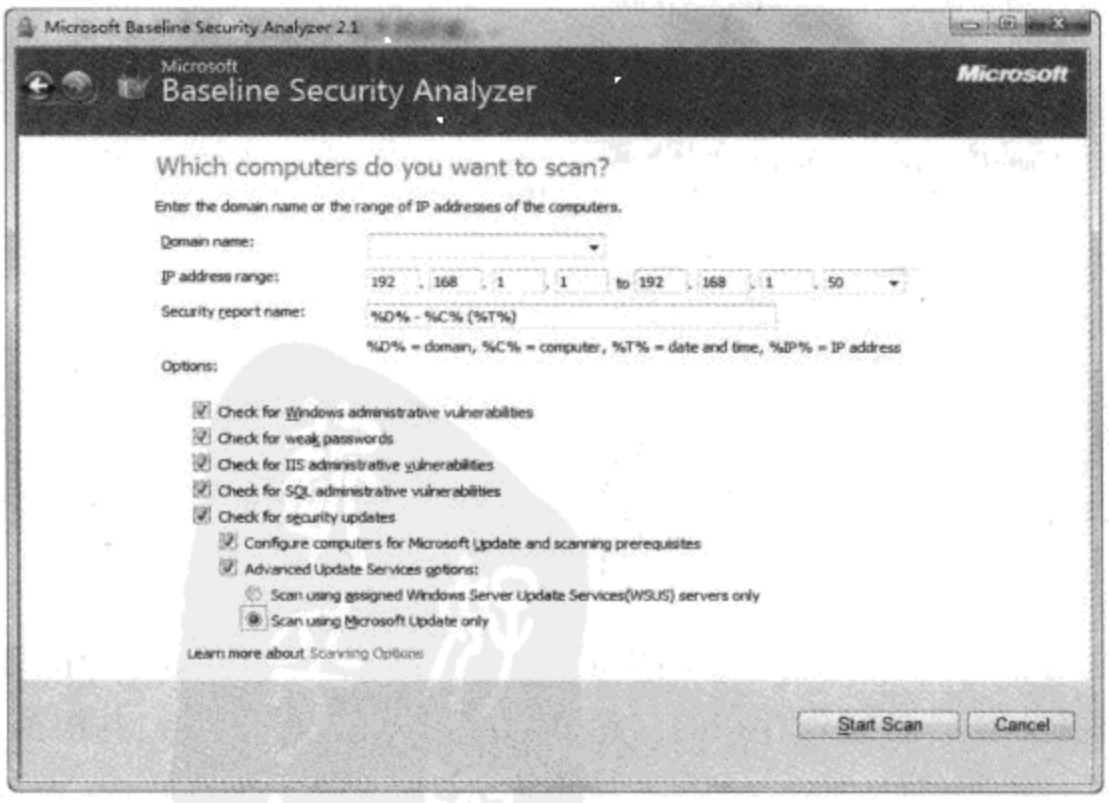


图 4-17　配置扫描选项

STEP 03 该工具可对整个域中所有的计算机进行扫描，或者也可以通过 IP 地址段指定需要批量扫描的计算机。因此，首先需要通过这两种方式中的任何一种指定需要被扫描的计算机。

STEP 04 随后需要注意“Options（选项）”部分的内容，MBSA 可以扫描 Windows 的管理漏洞、弱密码、IIS 配置问题、SQL 配置问题，以及安全更新的安装情况，这些都是默认选中的。如果不需要扫描某个内容，可以反选对应的选项。

STEP 05 如果局域网无法连接到互联网，则需要选中“Advanced Update Services options（高级更新服务选项）”，然后选中“Scan using assigned Windows Server Update Services servers only（仅使用分配的 WSUS 服务器）”，这样在扫描时，工具就会从本机使用的 WSUS 服务器上获得安全定义文件，而不需要访问互联网上的微软服务器。

STEP 06 设置好选项后单击“Start Scan（开始扫描）”，并耐心等待。如果选择的计算机比较多，或者网络比较繁忙，这个过程可能需要花费一些时间。

扫描结束后，通常可看到图 4-18 所示的结果。在默认的排序下，最严重的问题会被放在报告的最顶端。另外，通过不同的图标也可以了解不同的安全程度，如果图标显示为绿色的盾牌，表示该内容是安全的；如果是黄色的感叹号，则表示可能存在安全问题。对于每一项内容，还可以通过相应的链接了解具体的扫描内容，以及如何解决可能存在的问题。

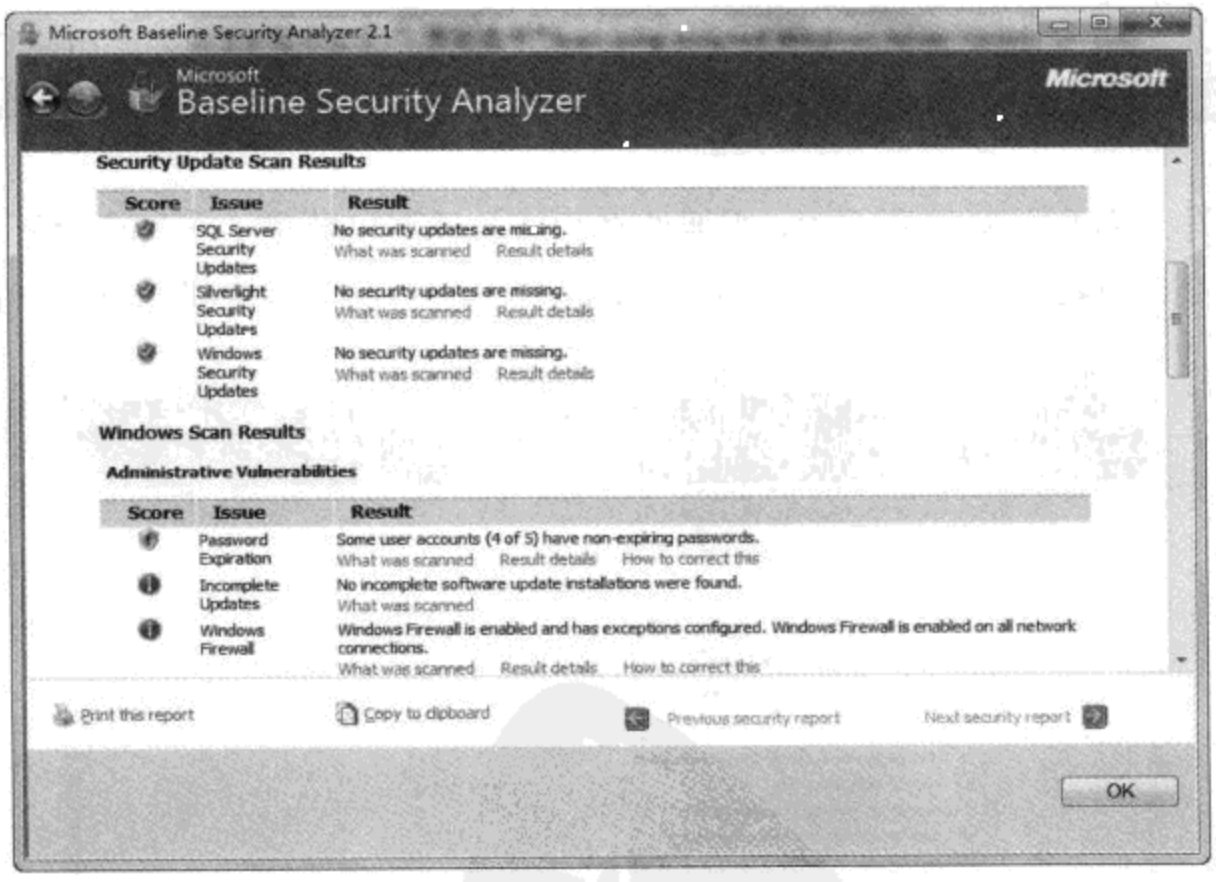


图 4-18　MBSA 的扫描结果

通过定期使用 MBSA 工具扫描环境中的所有计算机，管理员即可确保每台计算机的安全性是否符合预期。而一旦发现存在的问题，也可以做到心中有数，并根据 MBSA 的建议尽早解决。

CHAPTER

5

第 5 章　数据安全

在保证系统安全的同时，我们不能忽略数据的安全。毕竟很多人使用计算机都是用于工作的，要处理工作中用到的大量数据，对于这些人来说，计算机也就是一个最基本的工具罢了，丢失或者损坏可以接受，但数据的损失是不可接受的。因此，本章会告诉大家怎样在创建出一个安全的操作系统的同时保护好自己的数据安全。

5.1　NTFS 权限简介

计算机的硬盘是用于保存数据的主要设备，而硬盘在能够保存数据之前，必须创建好相应的分区或卷，同时使用一定的文件系统对分区或卷进行格式化操作。在这里面对数据安全影响最大的就是文件系统的选择。

对于目前的 Windows 操作系统，支持的硬盘文件系统主要有：FAT16、FAT32、NTFS，其中 FAT16 是最古老的，通常情况下，如果不考虑兼容性，基本上没有人会继续使用，大部分人现在使用的是 FAT32 和 NTFS 文件系统。

然而对于 Windows 7，情况有了一些变化，因为 Windows 7 要求必须安装在 NTFS 文件系统的分区上，这主要是为了保证系统的安全性，另外，上文还曾提到过，Windows 7 模块化的设计方式要求使用 NTFS 文件系统所提供的硬连接功能。但有很多人即使在使用 Windows 7，习惯上依然保留一两个 FAT32 的分区用于保存自己的文件。

现阶段，依然在使用 FAT32 文件系统的人所坚持的理由主要有以下几个：

- **FAT32 的兼容性好**　没错，如果希望使用 Windows XP/Vista/7 与古老的 Windows 9x 形成多重启动系统，那么保留 FAT32 分区是很有必要的。
- **FAT32 的故障恢复更好处理**　这种观点其实已经站不住脚了，这里所说的故障恢复，其实就是 DOS 下的访问，因为至今很多人依然离不开 DOS，一旦系统崩溃，为了挽救自己的数据，很多人还是习惯于使用 DOS 引导盘引导系统，然后使用 DOS 命令将文件复制出来。现在，Windows 本身就提供了很好的恢复环境，我们完全可以用它取代古老的 DOS。

- **NTFS 不支持 Ghost 等镜像备份软件** 这个观点更经不起推敲，从 Windows 2000 大规模普及的时代开始，Ghost 等镜像备份工具就已经开始支持 NTFS 文件系统的分区了，更何况 Windows 都已经发展了两代，目前市面上几乎所有的镜像备份和还原软件都支持 NTFS 文件系统的分区。不仅如此，在新版本 Windows 中，本身就包含了一套基于 Windows PE 的恢复环境，完全可以取代古老的 DOS 以及 Ghost 等第三方工具。

5.1.1 FAT32 和 NTFS 文件系统对比

FAT32 与 NTFS 文件系统对比就算不合适，我们又有什么理由非要使用 NTFS 呢？其实，NTFS 和 FAT32 相比，其优点在于：

- **NTFS 文件系统支持更大的文件以及更大的分区** FAT32 分区随着分区体积的增大，簇的大小也会逐渐增大，这会造成一定的空间浪费；而 NTFS 分区无论体积有多大，都可以保持 4KB 的簇大小，这样保存大量小文件的时候更有效率。另外，FAT32 分区保存的文件体积最大只能达到 4GB，而 NTFS 分区上的文件体积最大可以达到 16TB（1TB=1024GB）。
- **NTFS 分区支持权限设置** 我们可以根据实际情况对文件或文件夹的访问进行限制。FAT32 分区没有这一功能。
- **NTFS 分区支持 EFS 加密** 该功能可以配合权限一起使用，保证文件安全。FAT32 分区没有这一功能。
- **NTFS 分区支持压缩功能** 该功能可以节约零碎文件占用的硬盘空间。FAT32 分区没有这样的功能。
- **NTFS 分区的磁盘配额功能** 利用该功能，可以让我们限制每个用户可以使用的硬盘空间，从而防止了某个用户保存大量文件后导致硬盘可用空间低的情况出现。FAT32 分区没有这样的功能。
- **NTFS 分区支持动态盘功能** 这样我们可以创建类似 RAID 0 或者 RAID 1 的磁盘阵列，增强磁盘读写性能或者数据安全性。FAT32 分区没有这样的功能。
- **NTFS 分区的恢复日志功能** 该功能可以记录对文件的更改，这样如果在读写数据的时候出现故障（例如死机或者断电），可以在一定程度上保证数据的安全性。FAT32 文件系统不具备这样的功能。

基于上述原因，如果不是为了考虑和老系统的兼容性，一般都建议整个硬盘的所有分区都使用 NTFS 文件系统，毕竟这样更安全、稳定，也更能充分发挥新版本 Windows 的所有特性。

5.1.2　获得 NTFS 分区

如果打算使用 NTFS 文件系统的分区，实现方法有两种：格式化和转换。如果在未划分的硬盘空间上新建分区，建议在格式化的时候直接选择使用 NTFS 文件系统进行格式化；如果是已经创建好的，并保存了数据的分区，建议使用系统自带的 convert.exe 工具将其转换为 NTFS 文件系统，这样该分区上保存的文件也不会受到破坏。

1．将分区格式化为 NTFS 文件系统

要想将现有的硬盘分区格式化为 NTFS 文件系统（注意，格式化操作会导致目标分区上现有的数据全部丢失，请小心操作），请按照下列步骤操作：

STEP 01 在“开始”菜单中打开“计算机”，列出本机已经创建好的所有的硬盘分区。

STEP 02 在要格式化的分区上单击鼠标右键，选择“格式化”，随后可以看到图 5-1 所示的界面。

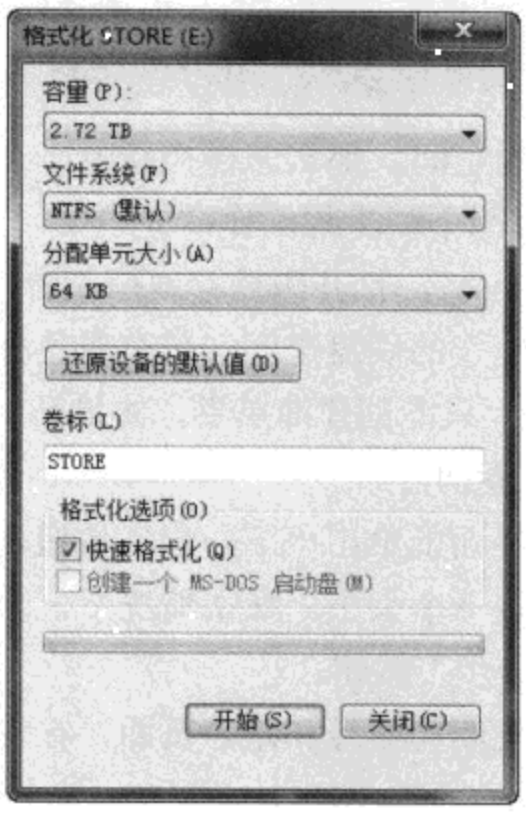


图 5-1　Windows 提供的格式化对话框

STEP 03 在“文件系统”下拉菜单中选择“NTFS”文件系统。这里需要注意，如果格式化的磁盘空间大小超过 32GB，那么 Windows 将限制只允许创建 NTFS 文件系统的分区，但实际上通过其他工具还是可以创建大于 32GB 的 FAT32 分区的。另外，“分配单元大小”决定了分区簇的大小，通常选择默认的“4096B”即可，或者也可以根据该分区的实际用途选择更大的簇。在“卷标”文本框中可以为该分区输入一个卷标，卷标主要用于标识该分区的用途。随后建议选中“快速格式化”选项，这样 Windows 会进行快速格式化，而不用检查硬盘，从而节约了时间（对于老硬盘，最好不要选择该选项，应让 Windows 彻底检查，以免硬盘有问题，日后危害数据安全）。

STEP 04 所有的选项都设置好之后，单击“开始”按钮，即可开始格式化该分区。

窍门 合理设置簇大小

对于簇的大小，很多人都有一个错误的认识，认为默认的 4KB 就挺好，其实并不是这样的。这里所说的 4KB，只不过是一个比较适合大部分情况的设置，然而这并不是万灵药。簇是硬盘上可以保存文件的最小单位，假设硬盘分区的簇大小是 4KB，而我们在硬盘上保存了一个 5KB 大小的文件，那么实际上该文件占据了两个簇，其中一个簇有 3KB 空间是没有被使用的。但是基于设计上的限制，这个簇中空闲的 3KB 空间无法被其他文件继续使用。因此，很早以前（主要是当时人们接触到的文件体积普遍不太大），人们觉得 4KB 的簇大小刚刚好。现在的情况是怎样的？上百兆字节甚至数吉字节大的文件也都很常见了，那么 4KB 的簇设置还合适吗？因此，我们完全可以根据分区的实际需要动态调整。例如，假如需要一个分区保存进行视频处理时的临时文件，这些文件体积都是很大的，那么完全可以设置更大一些的簇设置，这样磁头的读写才会更有效率。但如果需要一个分区保存文档文件，这时候使用 4KB 的簇设置是可以的。

如果硬盘上还有尚未划分的空间，那么怎样在新建一个硬盘分区的同时将其格式化为 NTFS 文件系统？这时候可以按照下列步骤操作：

STEP 01 运行“diskmgmt.msc”，打开磁盘管理控制台。

STEP 02 在显示为“未分配”的硬盘空间（带有黑色标记的空间）上单击鼠标右键，选择“新建简单卷”（在基本盘上只能创建简单卷，如果是动态盘，则可以创建跨区卷和带区卷），随后可以打开新建简单卷向导。

STEP 03 在向导的第一个界面上单击“下一步”按钮，随后可以看到指定卷大小的页面，在这里为需要创建的卷指定一个大小。默认情况下，这里会使用整个未分配的空间创建一个卷。设置好后单击“下一步”按钮。

STEP 04 随后可以看到分配驱动器号和路径页面，在这里可以决定该分区的盘符。设置好后单击“下一步”按钮。

STEP 05 随后可以看到图 5-2 所示的格式化分区界面，需要设置的内容都在这里。在这里设定好文件系统、分配单元大小（簇大小）、卷标，并决定是否执行快速格式化。

STEP 06 设置好所有的选项后单击“下一步”按钮，并复查设置。如果一切无误，就单击“完成”按钮，Windows 会按照我们的需要创建并格式化分区供我们使用。

2. 将分区转换为 NTFS 文件系统

如果希望将一个已经创建好，并且保存有数据的分区在不损坏数据的前提下转换为 NTFS 文件系统，这时候可以考虑使用 Windows 中自带的 convert.exe 工具。需要注意，该工具只能将分区无损地转换为 NTFS 文件系统，无法将分区由 NTFS 文件系统重新转换为 FAT32 文件系统。

Convert.exe 是一个命令行工具，因此，首先需要运行“cmd”启动命令行窗口，然后在该窗口中运行所需的命令。在 Windows 7 下使用时要注意 UAC 功能的影响，这时候必须使用管理员身份启动命令提示符窗口，方法是：打开“开始”菜单的“所有程序”子菜单，在“附件”下找到“命令提示符”快捷方式，用鼠标右键单击，选择“以管理员身份运行”。

假设需要将卷标为“DATA”的 E 盘转换为 NTFS 文件系统，打开命令提示符窗口后，请在命令提示符窗口中输入下列命令：

```
Convert e: /fs:ntfs
```

随后按照屏幕上的提示输入该分区的卷标，并按下回车键。当看到图 5-3 所示的界面时，表示转换操作已经完成。

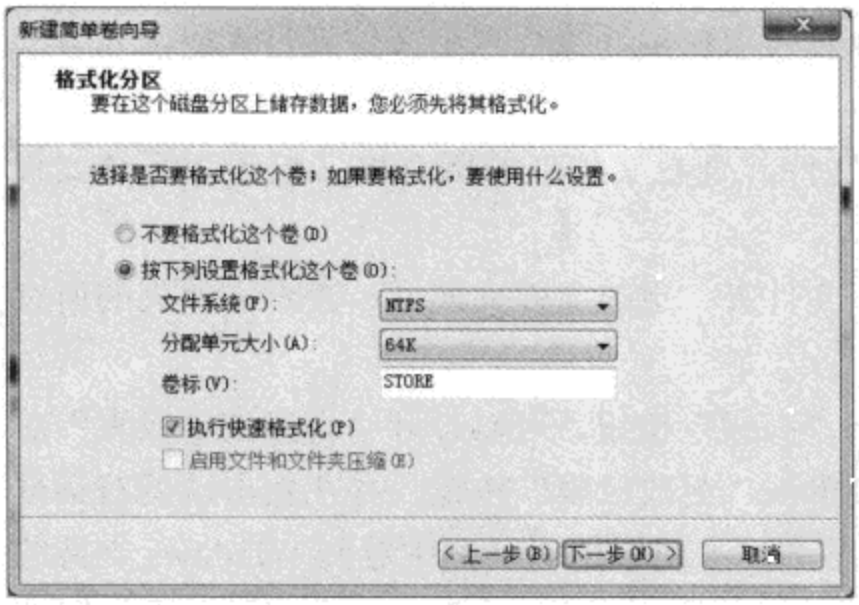


图 5-2　确定新建分区的各项参数

图 5-3　使用 convert 转换分区的文件系统

> **注意**　如果要转换的分区上有打开的文件，那么因为文件被锁定，转换将无法进行。因此，在转换前，请尽量关闭其他不需要的程序，或者在安全模式下进行。

另外，如果被转换的分区上包含分页文件或者其他重要的系统文件，转换操作可能必须重启后，在 Windows 载入之前进行。遇到这种情况时，屏幕上会有提示，我们只需要按照屏幕提示重启操作系统，即可完成转换操作。

5.2　NTFS 权限设置

有了 NTFS 分区后，我们就可以对其中保存的文件或文件夹设置权限。在设置之前，请注意两个问题：

- 操作系统的版本。只有 Windows 7 专业版/企业版/旗舰版才可以设置访问权限。
- 要按照 1.3.1 节新建账户并创建密码中的介绍为所有使用本机的人创建各自独立的用户账户，因为只有每个人使用自己的账户，才可以有效地控制访问。

要调整 NTFS 访问属性，需要在 Windows 资源管理器中用鼠标右键单击目标对象，例如硬盘分区、文件或文件夹，选择“属性”，打开“属性”对话框的“安全”选项卡，随后即可看到图 5-4 所示的界面。NTFS 访问权限就是在这里进行设置的。

在 Windows 7 中，因为 UAC 功能的存在，默认情况下，大部分设置都是只能查看，而不能直接修改。如果要修改设置，还必须单击相应的“编辑”按钮，根据当前登录用户权限的不同，可能还需要输入管理员账户的密码，随后才能继续操作。为了叙述方便，下文将不再重复提醒大家 UAC 的存在，实际操作时还需留意。

如图 5-4 所示，文件和文件夹的标准 NTFS 权限包括：

- **完全控制** 更改权限、接管所有权、删除子文件夹和文件、执行其他操作。
- **修改** 删除、执行写入权限、执行读取和执行权限允许的操作。
- **读取和执行** 浏览文件夹的内容、执行读取权限、执行列出文件夹目录权限允许的操作。
- **读取** 查看文件夹内的子文件夹和文件，查看文件夹的所有权、权限和系统文件属性。
- **写入** 在文件夹内创建新的文件和子文件夹、更改文件夹属性、查看文件夹的所有权和权限。

在图 5-4 所示的“属性”对话框中单击“高级”按钮，可以打开“高级安全设置”对话框，在该对话框的“权限”选项卡上直接单击“更改权限”按钮，并在新出现的对话框中任意单击列出的一则权限项目，随后可以在图 5-5 所示的对话框中看到 Windows 支持的所有高级权限（也就是所谓的“特殊权限”）。虽然大部分时候使用上文介绍的标准权限就能满足我们的使用需要，但有时候还得使用这些高级权限。

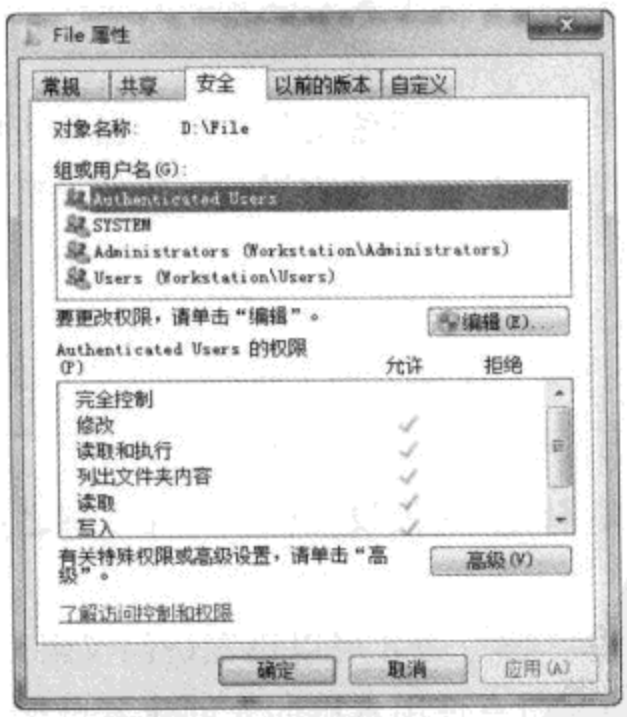


图 5-4 “属性”对话框的“安全”选项卡

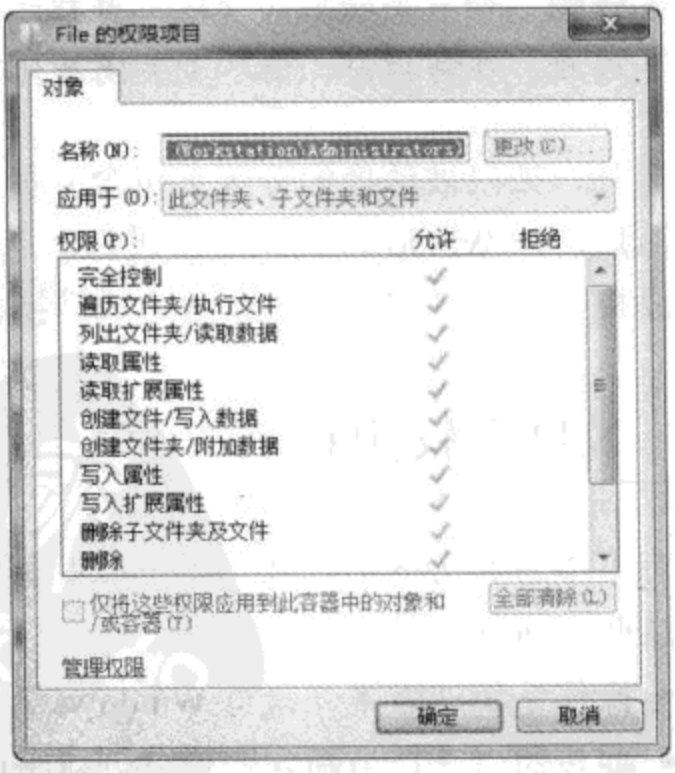


图 5-5 Windows 支持的高级权限项目

从图 5-5 中可以看到，Windows 支持的高级权限包括：遍历文件夹/执行文件、列出文件夹/读取数据、读取属性、读取扩展属性、创建文件/写入数据、创建文件夹/附加数据、写入属性、写入扩展属性、删除子文件夹及文件、删除读取权限、更改权限、取得所有权。

其实标准权限和特殊权限之间是有对应关系的，例如，标准权限中的“完全控制”就意味着具有其他所有的特殊权限。标准权限和特殊权限之间的对应关系请参考表 5-1。

表 5-1　标准权限和特殊权限的对应关系

特 殊 权 限	完 全 控 制	修　改	读取和执行	列出文件夹目录	读　取	写　入
遍历文件夹/执行文件	x	x	x	X		
列出文件夹/读取数据	x	x	x	x	x	
读取属性	x	x	x	x	x	
读取扩展属性	x	x	x	x	X	
创建文件/写入数据	x	x				x
创建文件夹/附加数据	x	x				X
写入属性	x	x				x
写入扩展属性	x	x				X
删除子文件夹及文件	X					
删除	x	X				
读取权限	x	x	x	x	x	x
更改权限	X					
取得所有权	x					

5.2.1　设置权限

假设需要针对一个文件夹“File”对名为“NewUser”的用户设置权限，希望该用户可以看到 File 文件夹中的文件名称，可以打开其中的所有文件，也可以修改其中的文件内容，但是不允许调整该文件夹的权限。操作步骤如下：

STEP 01 使用管理员账户登录，在 Windows 资源管理器中找到 File 文件夹，用鼠标右键单击，选择“属性”，打开“属性”对话框。

STEP 02 打开“安全”选项卡，单击“编辑”按钮。

STEP 03 在新出现的“File 的权限”对话框中单击“添加”按钮，打开图 5-6 所示的“选择用户或组”对话框。

STEP 04 在“输入对象名称来选择”文本框中输入“NewUser”，并单击“检查名称”按钮。如果输入正确，那么该用户的名称就会变成完整的“机器名\用户名”的形式。如果没有得到需要的结果，请单击“高级”按钮查找要设置的用户或组。

STEP 05 添加好用户或组之后单击“确定”按钮，返回“File 的权限”对话框，这时该对话框的组或用户名列表中就会新出现我们添加的“NewUser”用户（如图 5-7

所示）。

STEP 06 在组或用户名列表中选中该用户，然后在对话框下方“NewUser 的权限”列表中选择希望给该账户指派的权限。设置完成之后单击“确定”按钮即可。

在设置权限的时候，有人可能注意到了图 5-7 所示的内容，每个权限都有对应的“允许”和“拒绝”两个复选框。这两个复选框各自是在什么情况下使用的？在介绍这个问题之前，首先要提一下有关权限设置的一些规则，这些规则是：

- 权限是可以累加的。
- 拒绝权限优先于其他权限。
- 设置给文件的权限优先于设置给文件夹的权限。

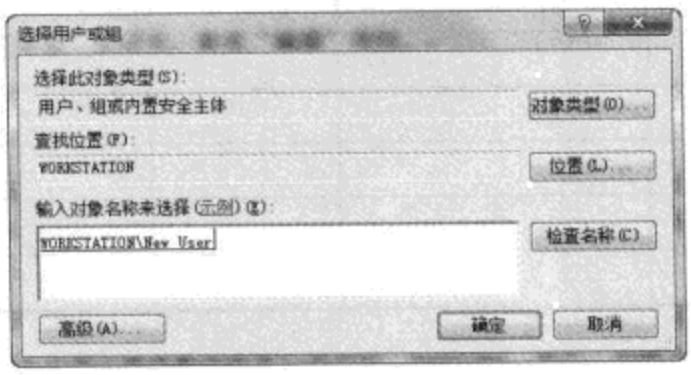


图 5-6 选择要设置权限的用户或组

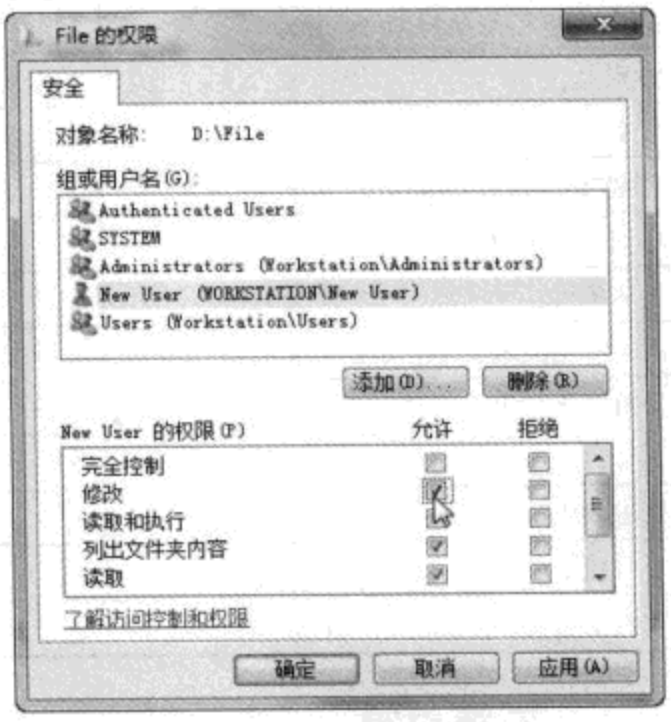


图 5-7 为选定的用户或组设置权限

下面逐一进行解释。

1. 权限是可以累加的

在上文中有人可能已经注意到了，在添加要设置权限的用户时，可以选择用户组。这也就意味着，我们不仅可以给用户，还可以给一个用户组设置访问权限，这样属于该组的用户就可以自动获得指派的所有权限（这正是使用用户组的初衷）。

有这样一种情况：假设一个用户“User”同时属于两个用户组：GroupA 和 GroupB。对于一个文件夹“Folder”，GroupA 具有读取和写入的权限；GroupB 具有读取的权限。那么，User 对 Folder 的真正权限是什么？因为权限是可以累加的，因此，在本例中，User 对 Folder 具有读取和写入的权限。

2. 拒绝权限优先于其他权限

上面的例子很好理解，那么换一种情况考虑，还是 User，他同时隶属于 GroupA 和 GroupB，存在一个 Folder，这一次 Folder 中保存有 FileA 和 FileB 两个文件。假设 GroupA

对 Folder 具有读取和写入的权限，但是 GroupB 对 Folder 中的 FileB 具有拒绝写入的权限。那么，UserA 对 FileA 和 FileB 的权限是怎样的呢？

这次的问题比较复杂，因为涉及到较多的权限关系和拒绝权限。首先考虑，因为 GroupB 对 FileB 被拒绝写入，因此，隶属于 GroupB 的 User 就会被拒绝写入 FileB，因为在这种情况下，拒绝权限是需要被优先考虑的。那么又因为 GroupB 对 FileA 的权限没有明确声明，从 GroupA 的关系来看，User 对 FileA 还至少应该具有读取和写入的权限。

在这里应该可以看出拒绝权限的用处了，虽然 GroupA 可以读取和写入 FolderA，但是属于 GroupA 的 User 却无法写入 FileB。

3．设置给文件的权限优先于设置给文件夹的权限

假设名为 User 的用户有一个文件夹 FolderA，其中保存有一个名为 FileA 的文件。此时，我们给 FolderA 设置权限，拒绝 User 的完全控制权限，但又给 FileA 设置权限，允许 User 读取。最终的结果是，尽管 User 无法直接在 Windows 资源管理器中双击打开 FolderA 文件夹，但他可以在地址栏中直接输入 FileA 的完整路径打开该文件查看内容。

也就是说，虽然文件夹的拒绝权限让这个用户无法查看文件夹中包含的内容（在 Windows 中，这一操作叫做“遍历”），但该文件夹中包含的文件的权限设置却允许用户直接访问文件的内容，只要该用户知道文件的完整路径即可。

5.2.2　判断有效权限

权限的设置是 Windows 中一个比较重要的操作，这个操作说起来很简单，但实际操作中却很麻烦，尤其是想要设置出不影响正常使用，但同时尽可能小的权限，还是很困难的。这往往需要反复测试和判断。那么，在给文件夹设置了复杂的权限后，如何判断一个用户对该文件夹或者文件夹中的文件具有怎样的权限？我们需要了解该用户的有效权限。

要判断某个用户或用户组对一个对象的有效权限，可以执行下列操作：

STEP 01 在要判断有效权限的对象上单击鼠标右键，选择“属性”，打开“属性”对话框，打开“安全”选项卡。

STEP 02 单击“高级”按钮，打开“高级安全设置”对话框，打开“有效权限”选项卡。

STEP 03 单击“选择”按钮，打开“选择用户或组”对话框，选择一个要查看有效权限的用户或用户组，单击“确定”按钮。

STEP 04 随后，“高级安全设置”对话框的“有效权限”选项卡下就会显示出该用户或用户组对该对象的有效权限，如图 5-8 所示。

- android与iphone及ipad开发书籍 ----------持续不断更新中.....
- c、c++、c#语言pdf书籍及vip视频教程 c、c++、c#、vc等-------持续不断更新中.....
- delphi《书籍》及《视频》教程 ----------持续不断更新中.....
- E网情深VIP系列视频教程 黑客破解菜鸟修练班，VB编程学习班，仿站学习培训，免杀培训，个人系统攻防系列教程，服务器搭建学习班，PHOTOSHOP平面设计班，基础制作论坛（论坛网站搭建），网赚系列教程，网站建设教程，网站漏洞基础，远程控制教程，软件破解班，脚本漏洞提权班
- IT9网络学院VIP系列视频教程 免杀培训班，VMware虚拟机，零基础学习C语言，网游外挂开发精品系列语音教程（外挂教程学习必备研修31课全），VB语言教程30课全，Delphi编程到精通，远程控制软件，加密解密班，网络安全与黑客攻防培训，从入门到精通完整系统化学习C++编程，从入门到精通零基础学习汇编，wordpress教程(个人博客系统49课全)，外行人做易语言盗号和钓鱼程序语音教程 网址：WLSAM168.400GB.COM
- Java书籍 ----------持续不断更新中.....
- photoshop、CorelDRAW、AutocAD等图像处理书籍及vip视频教程 -------持续不断更新中.....
- powerbuilder书籍大全
- Visual Basic语言vip视频教程及pdf书籍 ----------持续不断更新中.....
- windows、linux系统开发、系统封装等pdf书籍及VIP视频教程 ----------持续不断更新中.....
- 《3DS Max》pdf书籍
- 《汇编语言》、《反汇编》及《调试》pdf书籍及vip视频教程 ----------持续不断更新中.....
- 《电子书、电子书、还是电子书》pdf专题库 编程开发，家居美食，儿童益智，人物传记，增强记忆，快速阅读
- 信息系统项目管理师、网络工程师、系统分析师等软考类书籍
- 华中红客系列vip视频教程 脚本攻防培训班，源码免杀培训班，Css语言培训班，C语言，Dreamweaver网页设计，html网页设计培训班，PC安全班， php脚本语言培训班，VMWare虚拟机专题，webshell提权培训班，防站教程，零基础免杀培训班，刷钻速成班，脱壳破解班，外挂编写班，网络赚钱培训班，网站入侵培训班
- 外挂、驱动、逆向及封包视频教程 郁金香、独立团、夜猫论坛、天都吧、看流星论坛、一切从零开始等等
- 安全中国系列vip视频教程 易语言软件编程培训班，ASP.net网站开发项目实战培训班
- 我的收藏
- 按键精灵及TC脚本开发软件视频教程 ----------持续不断更新中.....

当前位置：/《电子书、电子书、还是电子书》pdf专题库

文件名 ⇕

PDF电子书专题库，内容详尽，每天不断更新！！

- 办公类软件使用指南
- 医学
- 历史人物传记
- 哲学宗教
- 外语资料（除英语外） （除英语外）
- 官场类小说
- 建筑工程类
- 情感生活类小说
- 政治军事
- 教育学习科普大全
- 文学理论
- 智力开发、增强记忆、快速阅读技巧大全
- 社会生活
- 科学技术
- 程序编程类
- 经济管理
- 网络安全及管理
- 网赚系列
- 美食小吃烹饪煲汤大全
- 课外读物

本网盘内容太多，持续不断更新，发布各类视频教程、pdf书籍，包括破解、加解密、外挂辅助制作，易语言培训教程、编程语言、网页制作等等，教程及书籍仅用于学习,如用于商业或非法用途的后果自负！

网址：WLSAM168.400GB.COM

- VIP培训教程，易语言黑月VIP视频教程，天都网易语言系列培训教程(100集全)，集中营易语言学习视频(80集)
- 棉猴系列vip视频教程 gh0st远控控制源码讲解教程，套接字编程，DLL程序编写，键盘监听驱动程序编写，驱动基础教程，AsyncSelect模型QQ程序教程，C++语言入门基础，NB5.5源码分析教程
- 游戏开发pdf书籍 ----------持续不断更新中.....
- 炒股投资pdf书籍及视频教程 短线高手系列，短线天王系列，操盘论道系列，翻倍黑马，看盘快速入门，庄家手法大曝光等等。 网址：WLSAM168.400GB.COM
- 热门小说集中营 傲世九重天，网游之三国时代，武动乾坤
- 甲壳虫VIP教程全集 asp教程，Delphi培训班，FLASH培训班，Java培训班，linux培训班，PHP培训班，源码免杀班，甲壳虫C++，脚本功防班，免杀班初、中、高级班，破解班，源码免杀班，脱壳班，易语言培训班，无特征码免杀，网站架构培训班，外挂高级班，外挂初级班第1、2部
- 破解、免杀、入侵、脱壳、攻防及漏洞分析系列VIP视频教程（80多部） 天草、黑客动画吧等等--------持续不断更新中....
- 网站建设相关的pdf书籍及各种vip视频教程 ----------持续不断更新中.....
- 网赚、淘宝系列vip视频教程 网赚30天新人魔鬼训练，屠龙网赚团队vip课程，站长大学网赚视频（50课全），图腾团队日赚1000元竞价行销教程，屠龙团队淘宝宝贝卖疯系列，站群网赚系列，淘宝开店视频，红星挂机日赚10元，百万流量系列，漂流瓶圣手全自动挂机引，贴吧邮件定向营销疯狂成交量月入万元
- 英语学习资料百科大全 不断更新。。。
- 饭客论坛系列VIP视频教程 脚本入侵班，黑客之免杀教程，易语言教程，无线网络攻防教程，入侵教程，delphi系列教程，黑客基础入门
- 黑客书籍 有关黑客、安全、加解密技术等等----------持续不断更新中.....
- 黑手安全网VIP系列视频教程 DIV+CSS网页布局，Dreamweaver教程，flsah动画教程，photoshop教程，跟我一起学C++课程，抓鸡
- 黑鹰、黑基、黑防、黑盾vip系列视频教程 破解提高班66课全，SQL注入，ASP注入教程，完完全全学会抓肉鸡，脱壳破解教程50课全，提权班，C语言特训班26讲全，黑客脚本特训班，黑客工具特训班，dedecms仿站教程，VC编写远控30课全，网页美工特训班，木马免杀特训班，驱动开发技术VIP培训班，外挂破解等等。

- [电脑世界的通关密语：电脑编程基础].(杉浦贤).滕永红.扫描版.pdf
- [程序语言的奥妙：算法解读（四色全彩）].(杉浦贤).李克秋.扫描版.pdf
- [差错：软件错误的致命影响].(帕伯斯).邝宇恒等.扫描版.pdf
- [算法之道（第2版）].邹恒明.扫描版.pdf
- [O'Reilly：深入学习MongoDB].(霍多罗夫).巨成等.扫描版.pdf
- [深入浅出WPF].刘铁猛.扫描版.pdf
- [Go语言·云动力（云计算时代的新型编程语言）].樊虹剑.扫描版.pdf
- [精通.NET互操作：P/ Invoke、C++ Interop和COM Interop].黄际洲等.扫描版.pdf
- [编程的奥秘：.NET软件技术学习与实践].金旭亮.扫描版.pdf
- [O'Reilly：学习OpenCV（中文版）].(布拉德斯基等).于仕琪等.扫描版.pdf
- [Go语言编程].许式伟等.扫描版.pdf 网址：WLSAM168.400GB.COM
- [MySQL技术内幕：SQL编程].姜承尧.扫描版.pdf
- [Tomcat权威指南（第2版）].(布里泰恩等).吴豪等.扫描版.pdf
- [Ext江湖].大漠穷秋.扫描版.pdf
- [IT名人堂·Oracle DBA突击：帮你赢得一份DBA职位].张晓明.扫描版.pdf

Total: 77 1 2 3 4 5 6 ›

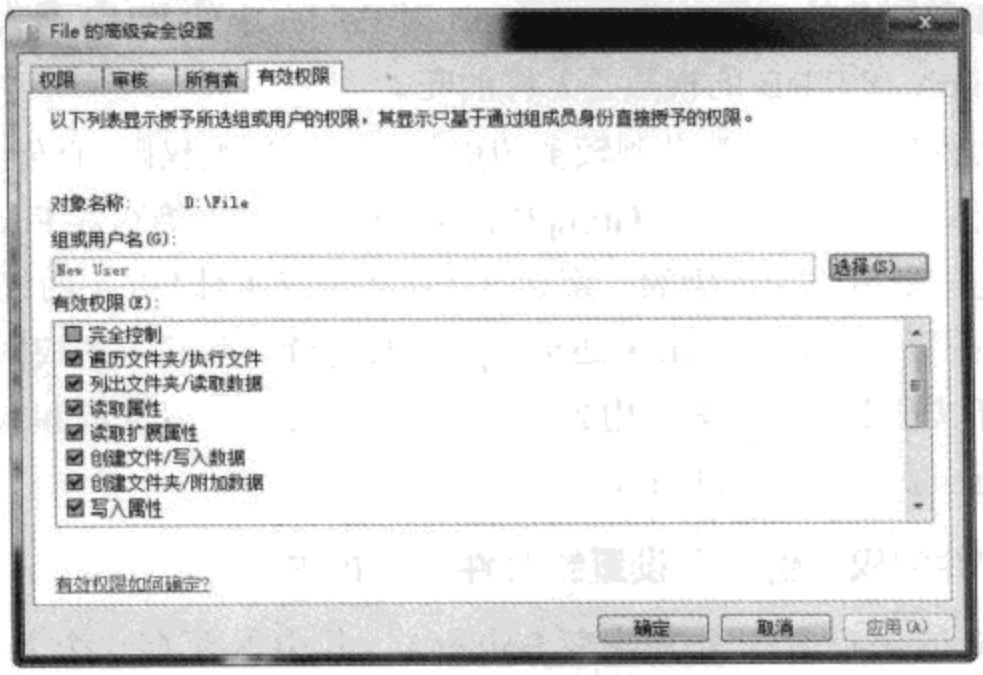


图 5-8　查看用户或组对某一特定对象所具有的有效权限

5.3　NTFS 权限高级应用

除了可以单独为对象设置权限外，我们还可以通过继承的方式获得权限。例如，有一个文件夹 Folder，其中有一个名为 File 的文件，默认情况下，我们设置给 Folder 的权限就会被自动应用给 File，同时我们在该文件夹下创建的其他子文件夹和文件都将自动获得设置给 Folder 的权限。简单来说，作为父文件夹，Folder 可以将自己的权限继承给子文件夹或者其中保存的文件。

另外，作为管理员，我们还可以按照需要为自己根本无权访问的文件重新指派权限或者指派所有者。

5.3.1　权限的继承

要了解权限的继承关系，请打开文件夹的“属性”对话框的“安全”选项卡，单击“高级”按钮，打开“高级安全设置”对话框的“权限”选项卡，随后可以看到图 5-9 所示的内容。

对比图 5-9 中左右两个对话框中的内容可以看到，左侧的组或用户名列表中显示了该文件夹被指派的不同权限，而从右侧对话框的权限项目列表中可以看到，只有为 NewUser 分配的权限是直接指派的（显示为“不是继承的”），而其他权限都是通过继承获得的。同时在右侧对话框的“应用于”一栏可以看出，这些权限不仅向上继承于父文件夹，而且还会向下继承给该文件夹的子文件夹。在具有继承关系的时候，我们对父文件夹的权限设置进行的任何修改都会被应用到继承的子文件夹和文件上。

如果希望中断继承关系，可以在图 5-9 右侧所示的对话框中单击“更改权限”按钮，然后取消对“包括可从该对象的父项继承的权限”选项的选择，随后可以看到一个“Windows

安全”提示框，如图 5-10 所示。

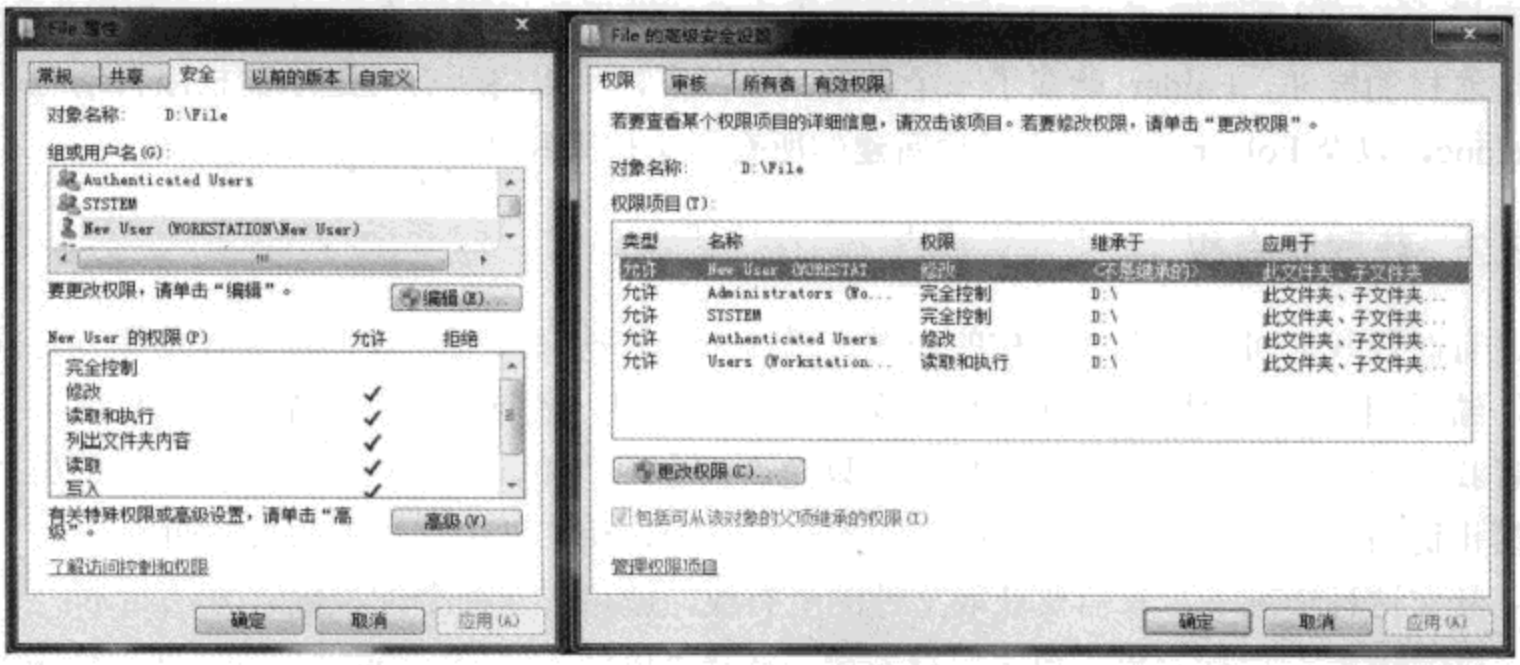


图 5-9　通过继承获得的权限

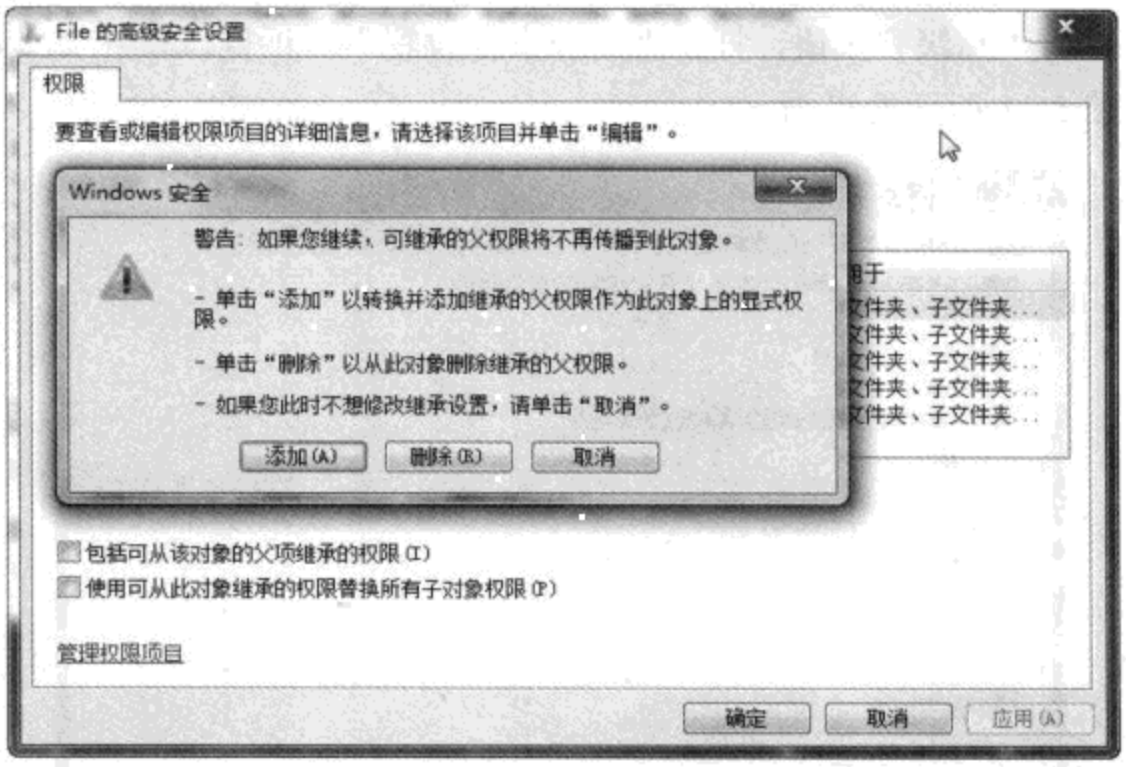


图 5-10　对权限的继承进行设置

在“Windows 安全”提示框中有三个选择：添加、删除和取消。

- 如果希望将父文件夹的权限设置复制给子对象，但同时断开继承关系，可以单击“添加”按钮，这样子对象依然会保留当时的权限设置，但继承关系已经中断。因此，随后对父文件夹权限的修改都将不会影响到子对象。
- 如果希望删除从父文件夹应用的所有权限，可以单击“删除”按钮，这样子对象继承来的所有权限设置都会被删除，但直接为子对象指派的权限会被保留。
- 如果是误操作，则可以单击“取消”按钮关闭该对话框。

除了断开和父文件夹的继承关系外，我们还可以让该子对象成为一个新的父对象。例

如，有这样的文件夹结构：\\file\folder\file.doc，当我们对其中的 Folder 文件夹断开了继承关系后，还可以选中图 5-10 中的“使用可从此对象继承的权限替换所有子对象权限”选项，经过这样的操作，Folder 就成了一个新的父文件夹，可以将所有可继承的权限自动应用于 File.doc，以及 Folder 文件夹中以后新建的所有子文件夹和文件。

5.3.2 获取所有权

有时候我们可能会面临这样的问题：系统中有一些文件夹，我们曾对其设置过访问权限，结果因为一些原因导致我们重新安装了操作系统，之前的那些文件就再也打不开了。或者我们曾对一个文件夹设置了权限，只允许一个用户访问，其他用户（包括管理员）都被禁止访问。可有一天我们无意中删除了这个账户，该文件夹就再无法被访问。

其实这种情况下，只需要获取文件的所有权，就可以重新分配权限。方法如下：

STEP 01 在目标对象上单击鼠标右键，选择“属性”，打开“属性”对话框，打开“安全”选项卡。

STEP 02 单击“高级”按钮，打开“高级安全设置”对话框，打开“所有者”选项卡，随后可以看到图 5-11 所示的界面。

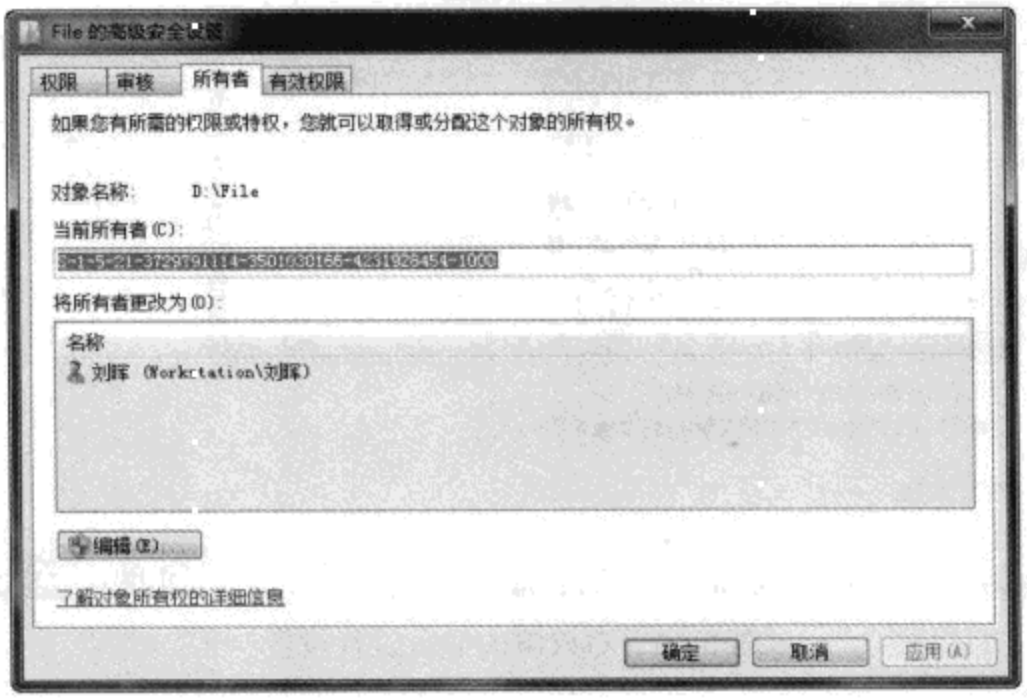


图 5-11 查看对象的所有者

STEP 03 注意“当前所有者”一栏显示的内容。正常情况下，这里会显示该对象的所有者的用户名，然而因为该文件夹是在以前的操作系统中创建的，我们重新安装了系统后，系统只能记住在以前系统中所有者账户对应的 SID（有关 SID 的详细信息，请参考 2.1.1.1 节安全标识符），而无法根据 SID 查询到用户名。我们希望将该文件夹的所有者改为当前系统中的某个有效账户，因此，直接单击“编辑”按钮，打开如图 5-12 所示的对话框。

STEP 04 首先从“将所有者更改为”列表中选择一个希望作为所有者的用户，或者单击“其他用户或组”按钮，选择其他用户或者用户组。接着选中“替换子容器和对象的所

有者”选项，因为只有这样才能更改该文件夹中的子对象的所有者。设置好之后单击“确定”按钮即可。

图 5-12　更改对象的所有者

STEP 05 在重新指派了所有者后，所有者已经可以访问文件夹了。如果希望其他用户也具有一定的访问权限，则可以按照上文介绍的方法进行设置。

5.3.3　权限设置的注意事项

权限的设置需要我们进行大量的练习，因为只有这样，才可以充分了解不同权限项目的作用，以及权限的应用方式。不过，在设置权限的时候，有以下注意事项需要了解：

- 只给目标对象分配必需的权限，其他非必要的权限尽量不要分配。毕竟最小的权限等于最大的安全。
- 通常情况下，尽量对文件夹设置权限，而不是对其中的某个文件设置权限。
- 在设置权限的时候，尽量针对用户组进行设置，而不是针对某个具体用户进行设置。
- 如果不希望某个用户或组具有某种权限，将其从权限列表中删除即可，一般情况下不需要添加明确的拒绝权限。
- 对象的权限是通过 SID 控制的，而非用户名。例如，如果创建了一个用户，为该用户给某个对象设置了权限，在删除该用户，然后使用同样的用户名和密码重建用户后，新建的同名用户并不能直接获得之前分配的任何权限。

5.4　EFS 加密

通过使用 NTFS 权限，我们可以控制用户对文件和文件夹的访问，然而仅仅这样并不能保证数据的绝对安全。

例如，为了保证数据安全，我们给一个文件夹设置了权限，只允许某个用户访问，其他用户都无法访问。在这种情况下，如果不知道该用户的密码，别人都将无法访问这些数据。但只要系统中还有管理员账户，管理员随时可以获取文件夹的所有权，并给自己分配权限，从而是可以访问这些数据。

即使这台计算机只有一个人使用，别人无法使用管理员账户登录，那么最简单的办法，只要给这台计算机上再安装一套操作系统，使用新操作系统中的管理员账户登录，一样可以获取所有权并分配权限。所以，单纯的 NTFS 权限并不能完全保证数据安全，这时候，我们可以使用 EFS 加密。

EFS（Encrypting File System，加密文件系统）最早出现在 Windows 2000 操作系统中，它可以把 NTFS 分区上的数据加密保存起来。EFS 是一种公钥加密体系，也就是说，在加密的时候，系统会使用当前用户的公钥将数据加密并保存到硬盘上，而在解密的时候，会用到该用户对应的私钥，将数据解密，供用户使用。

和其他加密软件相比，EFS 最大的优势在于和系统紧密集成，同时对于用户来说，整个过程是透明的。例如，UserA 加密了一个文件，那么就只有 UserA 可以打开这个文件。当 UserA 登录到 Windows 的时候，系统已经验证了 UserA 的合法性，这种情况下，UserA 在 Windows 资源管理器中可以直接打开自己加密的文件，并进行编辑，在保存的时候，编辑后的内容会被自动加密并合并到文件中。在这个过程中，这位用户并不需要重复输入自己的密码，或者手工进行解密和重新加密的操作。因此，EFS 在使用上非常便捷。

> **注意** EFS 是一种文件系统层面的数据加密算法，并且完全基于公钥体系。因此，正常情况下，只要一个用户使用正确的密码登录系统，就可以正常访问自己加密的所有文件。而很多人对于“加密”，希望做到的则是：要想双击打开一个被加密的文件，首先需要在弹出的对话框中输入正确的密码，随后才可以访问。这一点 EFS 是无法实现的。
>
> 另外，假设用户 A 加密了一些文件，用户 B 在登录系统后，虽然无法读取文件的实际内容，但只要 NTFS 权限允许，用户 B 依然可以看到用户 A 加密文件的文件名称和属性，甚至用户 B 可以删除这些文件。这属于 EFS 的设计特性。

完全支持 EFS 加密和解密的操作系统包括 Windows 7 专业版/企业版/旗舰版。Windows 7 家庭基础版/家庭高级版只能在有证书的情况下打开被 EFS 加密的文件，而无法加密新的文件。

5.4.1 加密和解密文件

文件的加密和解密操作是很简单的，我们只需要用鼠标右键单击想要加密或解密的文件或文件夹，选择“属性”，打开“属性”对话框的“常规”选项卡，接着单击“高级”按

钮，打开图 5-13 所示的“高级属性”对话框。

如果希望加密文件或文件夹，请选中“加密内容以便保护数据”；如果希望解密文件或文件夹，请取消选中“加密内容以便保护数据”，然后单击“确定”按钮即可。如果选择加密或解密的对象是一个包含子文件夹或文件的文件夹，那么单击“确定”按钮后，将看到图 5-14 所示的“确认属性更改”对话框。

在这里，我们可以决定将该属性更改应用给哪些对象。例如，如果希望同时加密或解密该文件夹的子文件夹和文件，可以选择“将更改应用于此文件夹、子文件夹和文件”；如果只希望加密或解密该文件夹，则可以选择“仅将更改应用于此文件夹”。

默认情况下，被加密的文件或文件夹在 Windows 资源管理器中会显示为绿色，提醒我们注意。如果不希望使用这一特性，可以按照下列方法更改默认设置：

STEP 01 打开“计算机”窗口，按下键盘上的“Alt”键，打开菜单栏。

STEP 02 在菜单栏中依次单击“工具”→“文件夹选项”，打开“文件夹选项”对话框，打开“查看”选项卡。

STEP 03 在高级设置列表中，取消对“用彩色显示加密或压缩的 NTFS 文件”选项的选择。

STEP 04 单击“确定”按钮。

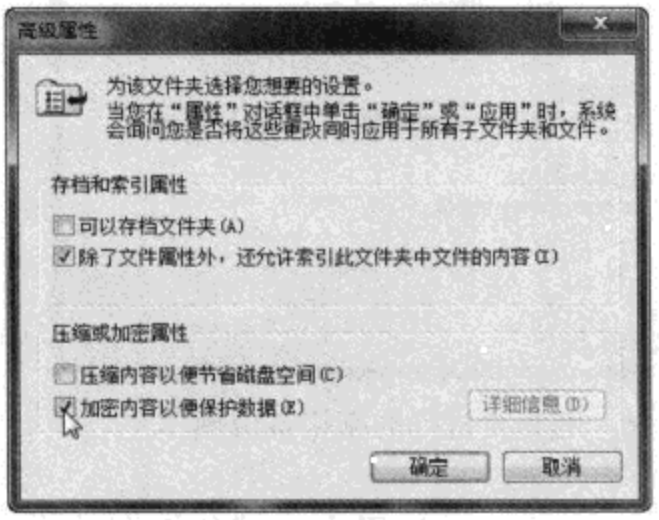


图 5-13　文件的加密和解密

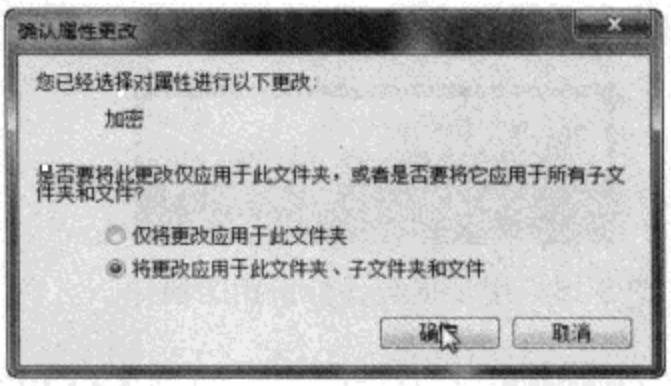


图 5-14　“确认属性更改”对话框

5.4.2　证书的备份和还原

上文已经介绍过，EFS 是一种公钥加密体系，因此，加密和解密操作都需要证书（也叫做密钥）的参与。但很多人都曾经遭遇过这样的情况：在系统中用 EFS 加密了文件，某天因为一些原因直接重装了操作系统，并创建了和老系统一样的用户名和密码账户，随后却发现自己之前曾经加密过的文件都打不开了。

如果仅仅是设置过 NTFS 权限的文件，还可以让管理员获取所有权并重新指派权限，但对于 EFS 加密过的文件，是没有解决办法的，因为解密文件所需的证书已经随着重装系统不存在了，在目前的技术水平下，如果想要在缺少证书的情况下解密文件，几乎是不可能的。

所以，要安全使用 EFS 加密，证书的备份和还原是一定要注意的。好在 Windows 7 会在我们第一次用 EFS 加密功能加密文件后提醒我们备份证书，而且操作也相对比较简单。

需要注意的是，每个人的证书都只有在这个人第一次用 EFS 加密了文件的时候才会自动生成，新创建的用户如果还没有加密过文件，是不会有证书的。因此，我们完全可以先加密一些临时文件，并立刻将证书备份起来，以便日后需要的时候还原。

1. 证书的备份

在 Windows 7 中，如果想要备份证书，可以这样操作：

STEP 01 在 Windows 7 中，当用户首次使用 EFS 加密文件或文件夹后，系统通知区域很快就会显示一个图标，并用气泡通知提醒用户注意备份自己的密钥（证书），如图 5-15 所示。

STEP 02 单击该通知后，可以看到图 5-16 所示的“加密文件系统”对话框，在这里有不同的操作可以选择。

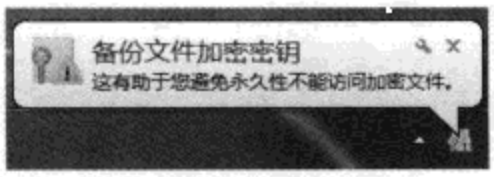


图 5-15　用于提醒备份密钥的通知

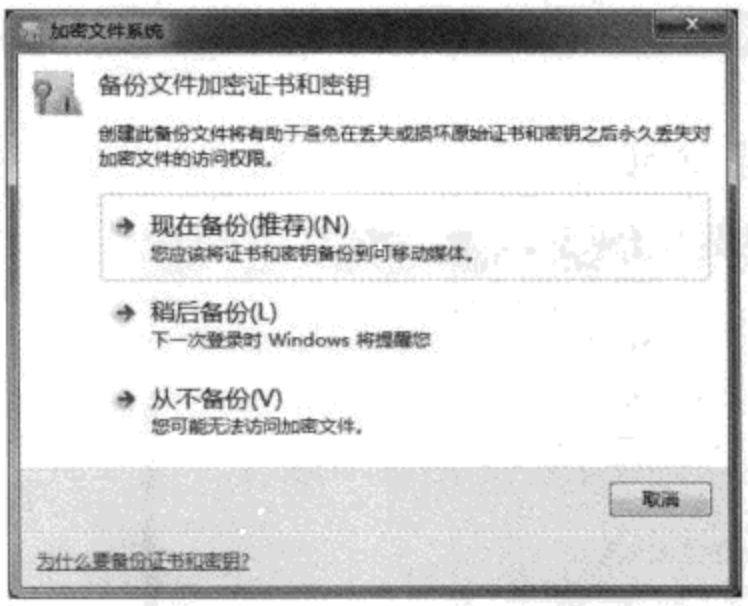


图 5-16　选择要进行的密钥备份操作

STEP 03 因为我们的目的是备份 EFS 加密证书，因此，直接单击“现在备份（推荐）”按钮，随后可以打开证书导出向导。

STEP 04 随后系统会打开密钥备份向导，我们只需要根据向导的提示，选择密钥备份文件的保存位置，并根据情况设置保护密码（这个密码一定要牢记，如果不知道这个密码，该备份的密钥将无法导入其他系统）即可。

导出的证书一定要保存在安全的地方，同时为了保险起见，最好能在不同的地方保存多个副本。

2. 证书的还原

要想将之前备份的证书还原到新的系统中，其操作非常简单，只要双击导出的.pfx 文件，系统就会自动运行证书导入向导，在向导的帮助下，我们只要输入导出证书时设置的

密码，即可完成导出操作。但在输入密码的时候有两个选项需要注意，如图 5-17 所示。

- **启用强私钥保护**　如果选中该选项，那么以后每次访问被加密的文件时，因为要用到私钥解密数据，系统都会向我们发出提示，提醒我们注意。
- **标志此密钥为可导出的密钥**　如果选中该选项，那么以后我们将可以从被导入的系统中将证书再次导出。如果导入私钥只是为了便于临时打开加密文件，则建议不要选择该选项。

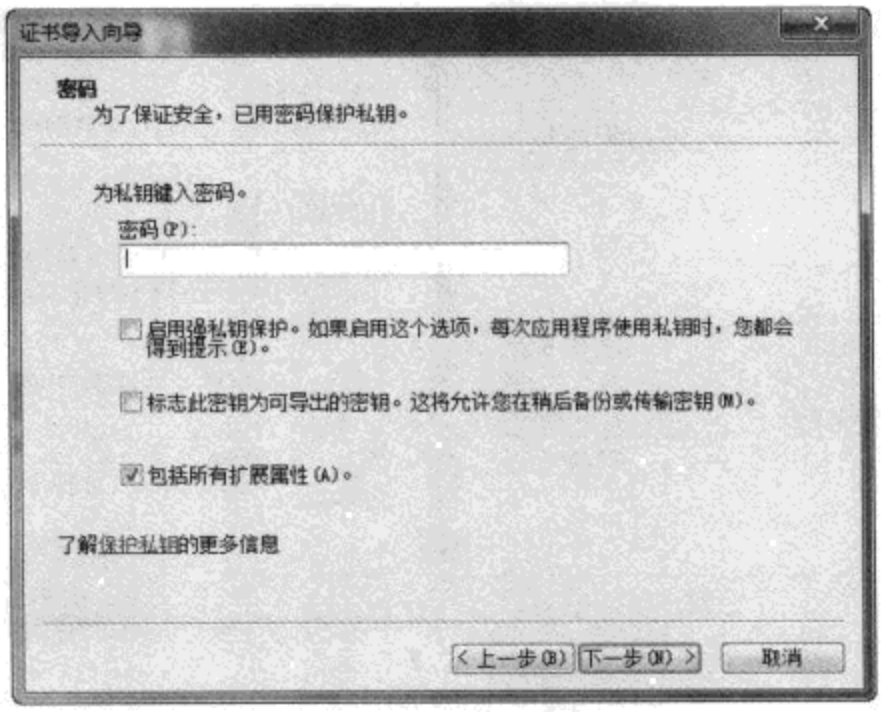


图 5-17　密钥的导入选项

5.4.3　EFS 的高级用法

上文已经介绍了 EFS 的基本用法，但在实际使用中，这些还是远远不够的。因为有些情况下，我们不仅要解决 EFS 令自己的数据更安全，还要保证一定的可用性。因此，下文会通过一些具体的示例告诉大家怎样用好 EFS 加密。

5.4.3.1　EFS 加密文件的共享

有时候，我们可能会希望实现这样的目的：同一个文件被加密后，可以被本机的两个用户使用，每个用户都可以查看和编辑文件的内容，但同时，文件依然处于被加密的状态。这种情况下，我们可以使用 EFS 的共享功能。

举例来说，具体环境是这样的：有两个用户 UserA 和 UserB，其中，UserA 在 E 盘根目录下创建了一个文本文件，输入了一些内容，保存后将其加密。我们需要做的是令 UserA 和 UserB 这两个用户都可以查看和编辑该文件，但其他用户无法打开。操作步骤如下（该方法仅适合文件，不适合整个文件夹）：

STEP 01　使用用户 UserB 登录，在桌面上创建一个临时文件，按照上文介绍的方法加密（这样做主要是为了生成 UserB 的 EFS 密钥，以便 UserA 设置 EFS 加密文件的共享）。

STEP 02　注销 UserB，使用 UserA 登录。打开 Windows 资源管理器，找到需要被共享

的 EFS 加密文件，用鼠标右键单击它，选择“属性”，打开“属性”对话框。

STEP 03 在“属性”对话框的“常规”选项卡中单击“高级”按钮，打开“高级属性”对话框，然后单击“详细信息”按钮，打开“用户访问”对话框，如图 5-18 左图所示。

STEP 04 单击“添加”按钮，打开图 5-18 右图所示的“Windows 安全”对话框，这里列出了本机上所有具有 EFS 密钥的用户，从中选择希望共享访问该 EFS 文件的用户，例如 UserB，然后单击“确定”按钮。

图 5-18　设置 EFS 加密文件的共享

STEP 05 随后在“用户访问”对话框的可访问这个文件的用户列表中就会显示两个用户。

STEP 06 日后，如果希望停止对某个用户共享该 EFS 加密文件，只需要打开“用户访问”对话框，从列表中选中目标用户，然后单击“删除”按钮，该用户访问这个加密文件的特权就会被删除。注意，该用户本身、该用户的证书，以及该用户共享访问其他 EFS 加密文件的特权不会受到影响。

STEP 07 单击“确定”按钮，关闭所有打开的对话框。

经过上述操作，用户 UserB 重新登录后就获得了打开该加密文件的特权。在使用该方法的时候需要注意，用户 UserB 将获得对该加密文件几乎全部的控制权，例如 UserB 和 UserA 一样，可以把其他用户添加进来，允许其他用户打开该文件。同时，UserB 也将可以禁止 UserA 打开该文件。因此，使用这个方法和别人共享 EFS 加密文件的时候一定要十分小心，以免给了别人访问的特权后，自己反而被别人排除在外。

5.4.3.2　加密可移动存储介质

上一节介绍的是如何在同一台计算机上共享 EFS 加密文件，那么，如何在不同的计算机上共享 EFS 加密文件呢？例如，公司员工可能需要将未完成的工作文件使用可移动存储设备带回家继续处理。为了防范存储设备失窃导致公司的机密数据泄露，我们可以将文件

用 EFS 加密后带回家，但怎样保证用户在家里的计算机上也能打开在公司计算机上加密的文件，同时在家里的计算机上编辑了文件后回到公司里也能打开？

具体环境是这样的：有两台计算机 A 和 B，A 在公司，B 在员工家里，这两台计算机都没有加入域。

STEP 01 在公司的计算机 A 上，将可移动存储设备格式化为 NTFS 文件系统，并在其根目录下创建一个文件夹，将所有需要带回家处理的文件复制到该文件夹中，并使用 EFS 加密该文件夹。

STEP 02 按照上文介绍的方法将用户的 EFS 加密证书备份出来，并随身携带（为安全起见，这个证书最好不要和被加密的文件保存到一起）。

STEP 03 在家里的计算机 B 上，按照上文介绍的方法，将公司里计算机 A 上备份出来的证书还原到家里的计算机 B 上。

STEP 04 将保存了机密数据的移动存储设备连接到计算机 B，查看并编辑文件，然后保存。

经过上述设置，在家里的计算机 B 上查看被 EFS 加密的文件属性，依然可以看到加密者是公司里的计算机 A 上自己的账户，但因为已经在计算机 B 上导入了计算机 A 上相应的证书，因此，打开和编辑这些文件都不是问题。就算在计算机 B 上编辑了这些文件，保存的时候，系统依然会自动以公司里计算机 A 上用户的身份加密所有的文件。因此，将编辑后的文件拿到公司后依然可以顺利访问。

5.4.3.3　使用恢复代理

在使用 EFS 加密时需要考虑的一个问题是加密所用的账户被删除后的文档恢复工作。例如，公司的计算机上有一个叫做“User”的账户，加密了一些机密信息。后来使用该账户的员工辞职了，因此，管理员直接删除了他的账户。但不久后，处理该账户的遗留文件时发现，该账户的一些文件还处于加密状态，而且这些文件全部无法打开。

前面已经提到过，Windows 是通过 SID 识别不同账户的，在这种情况下，重建相同用户名和密码的账户并不能得到原账户的 EFS 证书，因此，被加密的文件将无法解密。为了预防这个问题，微软在设计 EFS 加密功能的时候引入了一种叫做恢复代理（Recovery Agent）的机制。

> **注意**　SID 并不能代表一切
>
> EFS 密钥与用户的 SID 有很大关系，但 SID 并不是创建密钥的唯一条件。当用户首次使用 EFS 功能加密文件时，系统会结合用户的账户密码、SID，以及其他一些随机的参数一起创建 EFS 密钥。
>
> 因此，很多人在遇到由于重装系统导致密钥丢失，EFS 加密文件无法访问的问题后，可能会考虑，如果将新系统中账户的 SID 修改成老系统中一样的 SID，是否就可以恢复对 EFS 加密文件的访问。实际上，SID 虽然可以通过某些工具修改，但

> EFS 密钥是无法恢复的。因为密钥的创建除了需要参考 SID 外，还需要参考一些随机参数，SID 可以恢复，但随机参数是无法恢复的。
>
> 在使用 EFS 的时候，一定要注意密钥的保护，密钥丢失可能会导致灾难性的损失。网上流传着一个叫做 Advanced EFS Data Recovery（http://tinyurl.com/yanq3ua）的工具，可以用于破解被 EFS 加密的文件，但该工具的使用是有前提条件的。根据介绍，该工具可以逐扇区扫描硬盘，找出硬盘上保存的密钥，然后用于解密被加密的文件。该软件有效的一个前提就是：用于解密文件的密钥依然存在于硬盘上（这样的密钥就算无法通过正常途径读取也没关系，但一定要存在于硬盘上）。因此，如果是将硬盘转移到其他计算机上，可以使用该软件解密文件；如果格式化系统盘并重装系统，但密钥文件依然遗留在硬盘上（格式化后，密钥所在硬盘扇区只要没有被覆盖写入新的内容，依然可以恢复），用该软件也可以解决问题；如果格式化了硬盘分区，并且给分区中写入了大量新文件，将密钥所在扇区彻底覆盖，此时这个软件一样无法解密。

恢复代理可以理解为默认被共享了本机所有 EFS 加密文件的用户（类似于 EFS 的共享），在设置了恢复代理后，本机上所有的文件在使用 EFS 加密的同时，恢复代理的相应信息也会被保存到文件中。这样，日后就算加密该文件的账户已经不存在，或者证书丢失了，依然可以使用恢复代理的账户登录系统，并解密文件。

为了安全起见，在单机和工作组环境下的 Windows XP/Vista/7 中，默认情况下，没有恢复代理（单机环境的 Windows 2000 有 EFS 默认恢复代理：系统内建的 Administrator 账户）。在加入域后，默认的恢复代理是域管理员。因此，首先需要为系统指定一个恢复代理。

STEP 01 使用希望成为恢复代理的账户（最好是管理员账户）登录，然后在该账户的桌面上创建一个临时文件，例如“1.txt”。

STEP 02 运行“cmd”，打开命令提示符窗口，然后使用“cd desktop”命令进入到该账户的桌面文件夹下。

STEP 03 运行命令 cipher /r:1.txt，随后输入用于加密证书的密码（注意，在输入的过程中，光标并不会有变化，也不会用星号代表输入的密码位数），如图 5-19 所示。随后在桌面上会看到一个名为“1.cer”的文件，我们可以通过该文件将当前登录的用户指定为恢复代理。

```
C:\Users\liuhui\Desktop>cipher /r:1.txt
请键入密码来保护 .PFX 文件:
请重新键入密码来进行确认:


.CER 文件已成功创建。
.PFX 文件已成功创建。

C:\Users\liuhui\Desktop>_
```

图 5-19　生成指定恢复代理所需的用户密钥

STEP 04 运行“secpol.msc”，打开本地安全策略控制台。在控制台窗口左侧的树形图中依次进入到“安全设置”→“公钥策略”→“加密文件系统”。

STEP 05 用鼠标右键单击“加密文件系统”节点，选择“添加数据恢复代理程序”命令，打开添加故障恢复代理向导。

STEP 06 在向导的第一个界面中单击“下一步”按钮，在随后出现的界面上单击“浏览文件夹”按钮，并找到在第一步备份出来的证书 1.cer。

STEP 07 在导入的过程中，Windows 可能会提示 Windows 无法判断此证书是否被吊销，询问是否继续。在单机或者工作组环境下这是正常的，可以不用理会。

STEP 08 随后可以看到，添加故障恢复代理向导中已经列出了一个恢复向导，这表示操作是正确的（如图 5-20 所示），单击“下一步”按钮，然后单击“完成”按钮。如果需要，也可以添加多个恢复代理。

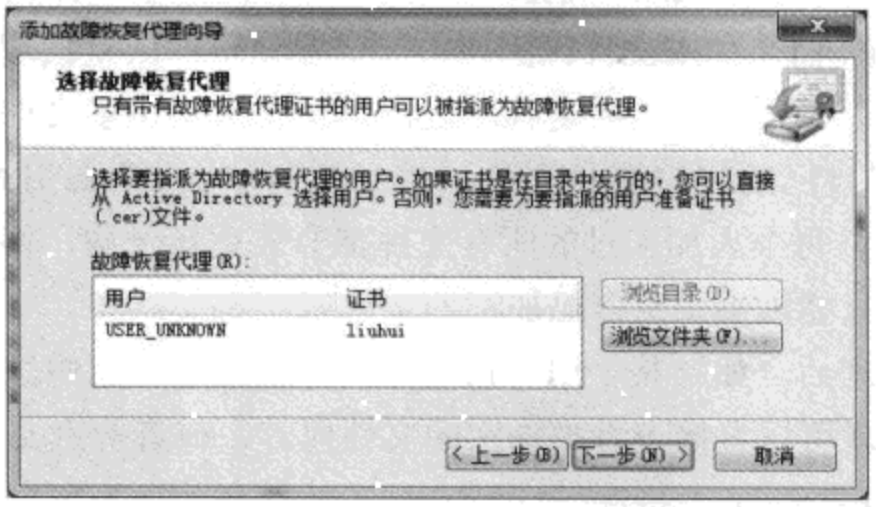


图 5-20　添加好的恢复代理

STEP 09 经过上述设置，在本地安全策略控制台的“加密文件系统”节点下会显示本机指定的所有的恢复代理，这表示当前本机已经具有了恢复代理，但操作还没有全部完成。

STEP 10 为了让恢复代理能够打开每个用户的加密文件，或者将其解密，还需要导入恢复代理的证书。依然使用恢复代理的账户登录系统，然后双击步骤 3 中生成的“1.txt.pfx”文件，将该证书导入。

STEP 11 如果导入成功，那么运行 certmgr.msc 打开的证书控制台中，在“证书当前用户”→“个人”→“证书”节点下应该能看到一个“预期目的”为“文件恢复”的证书。如果看到该证书，表示恢复代理的设置工作全部完成。

现在使用本机的其他账户登录，并加密一些文件，然后打开“被加密文件的用户访问”对话框，可以看到图 5-21 所示的界面。与图 5-18 显示的内容对比可知，那时候的恢复代理还是空的。

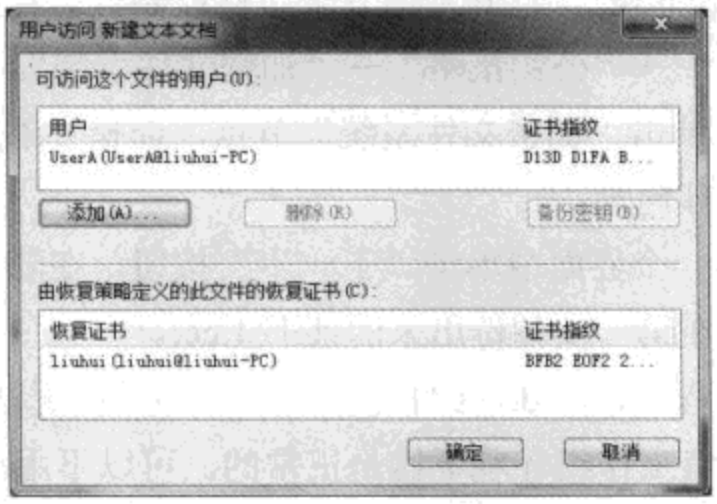


图 5-21　新加密的文件已经包含恢复代理的相关信息

使用恢复代理的时候需要注意，假设有位用户在指定恢复代理之前就已经加密了自己的文件，而随后才指定了恢复代理，那么，一旦该用户被删除或者 EFS 证书丢失，恢复代理将无法解密该用户的 EFS 加密文件。因此，一定要记住：恢复代理只能解密被指定之后其他用户加密的文件。如果在指定恢复代理之前已经加密了很多文件，那么每个加密过文件的用户都需要使用自己的账户登录系统，然后运行“cmd”打开命令提示行，并运行“cipher /u”命令，这样每个人加密过的所有文件都会被更新一次，将恢复代理的信息加入进去（每个人的操作只能影响到由自己加密的文件）。

在设置好恢复代理后，如果某个用户被删除，或者证书无意中丢失，只要被加密的文件还存在，恢复代理就可以直接查看被加密的文件内容，或者解密文件。

5.4.3.4　EFS 的使用注意事项

EFS 的功能很强大，虽然使用过程很简单，但需要注意的事项却有很多，如果不够注意，很可能会让自己永远都无法打开曾被加密过的重要文件。因此，在正式投入使用之前，请先注意下列问题。

1．永远先进行测试

无论打算借助 EFS 实现怎样的功能，一定要记住，在正式应用之前，需要先进行测试。否则，不仅无法保证数据的安全，还有可能导致自己都无法解密自己数据的情况出现，造成更大的损失。

2．将 EFS 加密和 NTFS 权限配合使用

EFS 加密只能保证自己的重要文件数据不被偷窥，但并不保证文件本身的安全。例如，我们在计算机上加密了一个文件，别人自然是看不到文件的内容，但别人可以删除这个文件。就算没有权限，只要使用管理员账户登录（可以破解管理员账户的密码，或者干脆给计算机中再安装一个操作系统），就可以获得所有权，并分配访问权限。不过，在这种情况下，对方依然看不到机密文件的内容，但完全可以将其删除。因此，最好同时配合备份功能对重要数据进行备份。有关备份的详细信息，请参考本书第 13 章。

3. 加密证书的创建时间

很多人还曾遇到过这样的问题：安装好系统和应用软件，并设置好所有的选项后，使用镜像备份软件（例如 Ghost）对系统进行了完整备份。然后开始使用系统，并用 EFS 加密了文件。一段时间后，系统出现了问题，于是，使用之前的备份将系统还原为备份时的状态，但发现自己的 EFS 加密文件打不开了。

这个问题涉及 EFS 加密证书的创建时间问题。和很多人想象中的不同，EFS 加密证书并不是在创建用户账户的时候进行的，而是在账户第一次加密文件的时候创建的。在对系统进行备份的时候，如果还没有用 EFS 加密过文件，那么，这时候系统中并没有 EFS 加密证书，系统的备份文件中也不会有，使用这样的备份文件还原系统后，因为没有证书（虽然是同一个用户账户，同样的 SID，同样的用户名和密码），因此，无法打开自己加密的文件。

4. 添加快捷菜单项

每当要用 EFS 加密或解密文件的时候，都需要用鼠标右键单击文件，选择“属性”，然后在“文件属性”对话框中进行，这样相当麻烦。如果需要经常加密或解密文件，那么可以直接将加密和解密的命令添加到 Windows 资源管理器右键菜单中。

运行 regedit 打开注册表编辑器，定位到 HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/Advanced，在这里新建一个名为“Encryption ContextMenu”的 DWORD 值，将其数值设置为“1”。修改后，当我们在 Windows 资源管理器中用鼠标右键单击一个未加密的文件或文件夹后，右键菜单中就会出现加密的选项；如果鼠标右键单击的是加密过的文件或文件夹，那么右键菜单中就会出现解密的选项。

5. 禁用 EFS 加密

虽然 EFS 加密很好用，但并不是所有的人都需要。如果计算机是几个人共用的，如果不了解该功能的人无意中加密了文件，而忘记了备份证书，那么在证书丢失或者损坏后，会导致数据丢失。

因此，如果不需要使用 EFS 加密，也可以将其禁用。运行 regedit 打开注册表编辑器，定位到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ EFS，在这里新建一个名为“EfsConfiguration”的 DWORD 值，将其数值设置为“1”，这样，本机的 EFS 加密就被禁用了。日后，如果需要重新启用 EFS 加密，只需要将该值的数值改为“0”即可。

5.5　Office 文档安全

除了可以使用 NTFS 权限和 EFS 加密功能保护我们的机密数据外，还有一类文档类型的安全需要注意，那就是由 Microsoft Office 办公软件创建的文档。

例如，我们可能创建了一份文档需要给同事查看，但只希望查看文档的内容，不允许对文档进行任何修改，或者不允许打印这份文档。这些该如何实现呢？或者希望对自己创建的文档设置密码保护，只有知道密码的人才可以打开文档。

在所有版本的 Microsoft Office 软件中都有使用密码保护文档的功能，不过这个功能的作用很有限，能实现的限制也不多。最重要的是，网上有很多软件可以破解这种受到密码保护的 Microsoft Office 文档。因此，本书只打算对这个功能进行一些简单介绍，并将重点放在从 Microsoft Office 2003 之后才增加的 IRM（Information Rights Management，信息权利管理）上。下文将以 Microsoft Office 2010 的 Word 组件为例进行介绍。

5.5.1 使用密码保护文档

该功能适用于各种版本的 Microsoft Office 软件。当编辑好文件，需要保存或者另存为的时候，在打开的“保存或另存为”对话框中，单击“保存”按钮左侧的“工具”下拉菜单，并在随后出现的弹出菜单中选择“常规选项”命令，就可以看到图 5-22 所示的“常规选项”对话框。在这里可以设置两个密码：打开密码和修改密码。如果设置了打开密码，当双击这个文件试图打开的时候，Office 首先会弹出一个对话框，要求在“打开文件时的密码”文本框中输入密码，然后才能打开；如果设置了修改密码，当打开这个文件的时候，Office 会要求输入修改密码，如果不能输入修改密码，文件将以只读模式打开，无法编辑（如图 5-23 所示），只有输入正确的修改密码后，才可以打开编辑模式。

图 5-22 为 Office 文档设置密码保护

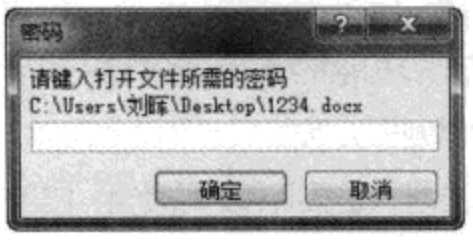


图 5-23 打开文档时需要输入修改密码

该功能的使用非常简单，但是需要再次提醒读者注意，这个功能并不是为了保护数据安全，只是为了防止文档编辑完后的误操作，而且网上有很多工具软件可以破解此类密码。如果希望对文档进行加密，并控制谁可以打开这些文件，以及哪些人可以对这个文件进行哪些操作，就需要参考下文介绍的 IRM 保护功能。

5.5.2 使用 IRM 保护文档

在介绍 IRM 功能之前，首先需要明确一个问题。Office 软件中的 IRM 功能最佳的使用

环境应该是具有 IRM 服务器的企业网络，因为在这样的环境下，整个企业可以在内部网络完成权限的确认、申请，以及设置和撤销等操作，安全性更高，同时凭据的验证还可以与 Windows 账户紧密集成。然而这一套系统需要不小的投入，相关的设置和管理也很复杂，一般情况下，只有大规模的企业用户才会考虑。

微软为了让一般用户也有机会体验 IRM 功能，为所有的用户提供了通过互联网使用的 IRM 管理服务。任何人只要有一台可以访问互联网的计算机，并拥有 Windows Live ID，就可以免费使用该服务。对于个人用户以及规模不是很大的中小企业用户，使用微软提供的免费服务显然更划算，也更方便。本节将以微软提供的免费服务为例进行介绍。

在继续阅读下文之前，请确保已经有一个 Windows Live ID。如果有@msn.com 或者@hotmail.com 的电子邮件账号，直接使用这个账号和密码即可。如果还没有，请在 http://account.live.com 页面免费申请。申请过程如下：

STEP 01 用浏览器访问 http://account.live.com，单击页面左侧的“注册”按钮。

STEP 02 在随后出现的页面上输入自己的个人信息和注册信息，并完成注册过程。这一过程与其他网站的注册基本上相同。

STEP 03 在注册时可以选择自己 Live ID 的后缀（例如@hotmail.com 或@live.cn），也可以单击“或使用您自己的电子邮件地址”链接，将自己的其他邮件地址注册为 Live ID。

STEP 04 如果使用自己的其他邮件地址进行注册，有两个问题需要注意：首先，因为输入了非微软提供的邮箱地址，为了确保申请人就是这个邮箱的主人，微软会向这个邮箱发送一封确认邮件，我们需要按照邮件中的说明完成确认操作。另外，用其他邮箱账号注册的 Live ID 并不等同于这个邮箱账号，假设用自己的 myemail@email.com（这是一个虚构的地址）注册为 Live ID，那么登录这个邮箱的密码是在注册邮箱的时候输入的，而登录 Live ID 的密码是在注册该 Live ID 的时候输入的，这两个密码可以不一样，同时也建议使用不同的密码。

STEP 05 根据网页上的提示完成剩余的注册过程，并记住账号和密码。

5.5.2.1　创建 IRM 保护的文档

现在我们看看怎样用 IRM 保护自己的文档。在此之前，首先要注册相应的服务，完整的过程如下：

STEP 01 单击 Word 窗口左上角的“文件”按钮，在弹出的菜单中单击“保护文档”，然后指向“按人员限制权限”，单击“管理凭据”（如图 5-24 所示），随后会出现服务注册向导。

STEP 02 在向导的第一个页面上选择“是，我希望注册使用 Microsoft 的这一免费试用服务”，单击“下一步”按钮。

STEP 03 在随后出现的页面上选择“是，我有 Windows Live ID”，然后单击“下一步”按钮。当然，如果还没有注册 Live ID，也可以选择“否”选项，随后还有一次注册的机会。

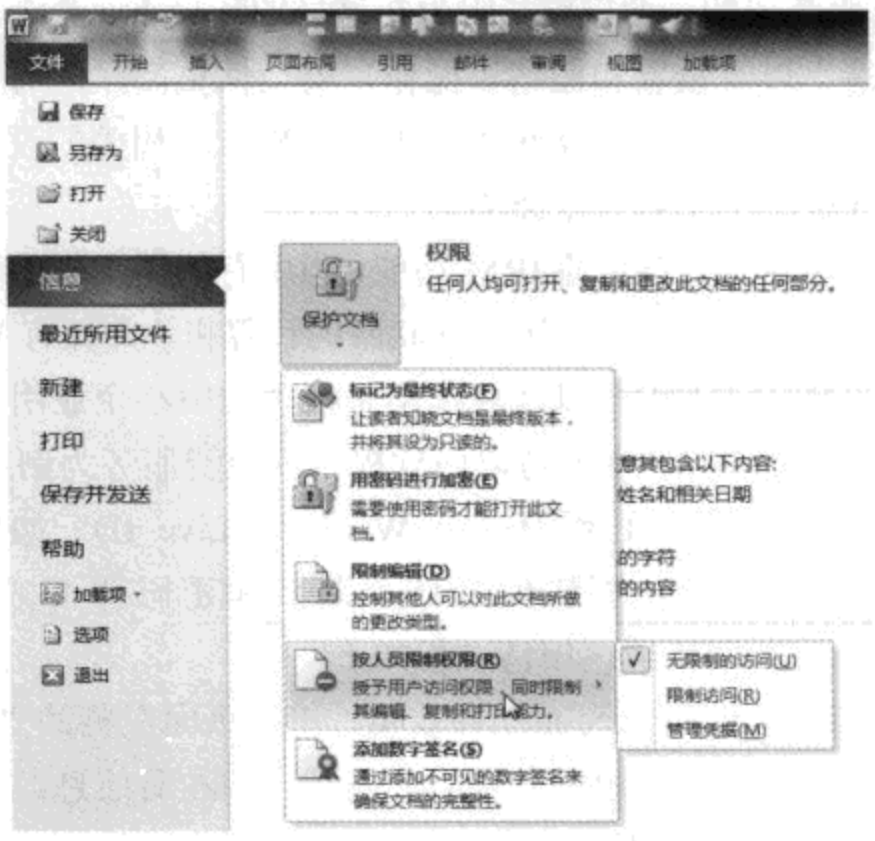


图 5-24　为 Word 文档设置 IRM 权限

STEP 04 输入 Windows Live ID 以及密码，然后单击“登录”按钮。如果需要，还可以选中“保存电子邮件地址和密码”，以免以后每次使用都需要再次登录。

STEP 05 随后选择本机的类型。可选的类型有“私人计算机”和“公用计算机”，对于每种类型的特点和适用范围，在对话框中都有详细的介绍（如图 5-25 所示）。根据实际情况选择合适的类型，然后单击“我接受”按钮。

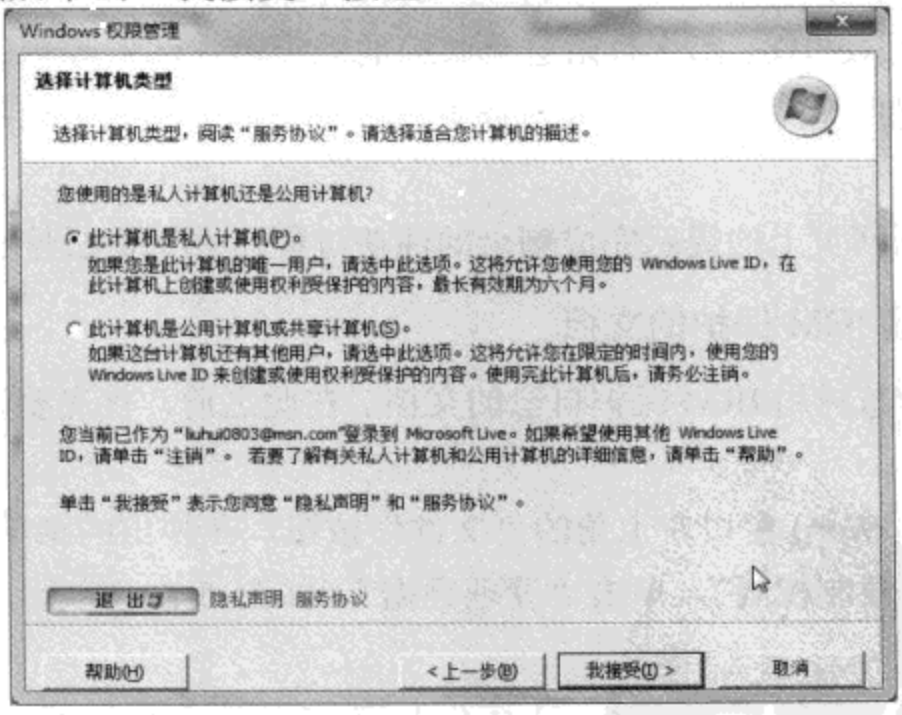


图 5-25　选择计算机的类型

STEP 06 选择好后，程序会用一段时间将证书下载到本地。下载好后单击“完成”按钮退出。这时候请注意证书的说明，取决于所选的计算机类型，获得的证书所能用于的计

算机数量会有不同限制。也就是说，假设我们创建了一个受 IRM 保护的文档，最多只能在一定数量的不同的设备（台式机、笔记本电脑或者手持设备等）上以“作者”的身份打开它。至于具体的数量，则取决于计算机是“公用”还是“专用”。另外，证书还有不同的寿命。

到这里，IRM 的设置工作就已经完成了。我们可以开始创建自己的文档，输入需要的内容，设置想要使用的格式和版面。当文档的编辑工作完成后，可以开始设置权限。这时候我们还是要单击 Word 窗口左上角的“文件”按钮，在弹出的菜单中单击“保护文档”，然后指向“按人员限制权限”，单击“管理凭据”，随后可以打开图 5-26 所示的“选择用户”对话框。

这里设置的是文档的作者，也就是对文档具有完整控制权的人，并且一份文档只能有一个作者。如果当前 Windows 账户只有一个人使用，那么也可以选中“始终使用此账户”，这样，以后该账户如果要使用 IRM 保护文档，就可以直接成为文档的作者，而不需要重新添加和选择。

在设置好作者后，还可以看到图 5-27 所示的对话框，在这里可以根据需要为不同的人添加“读者”权限。

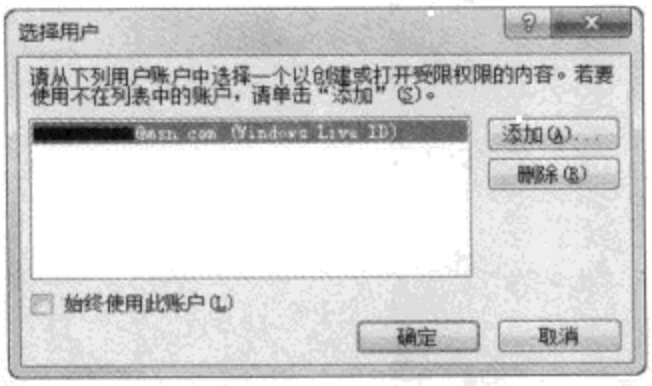


图 5-26　选择该文档的“作者”

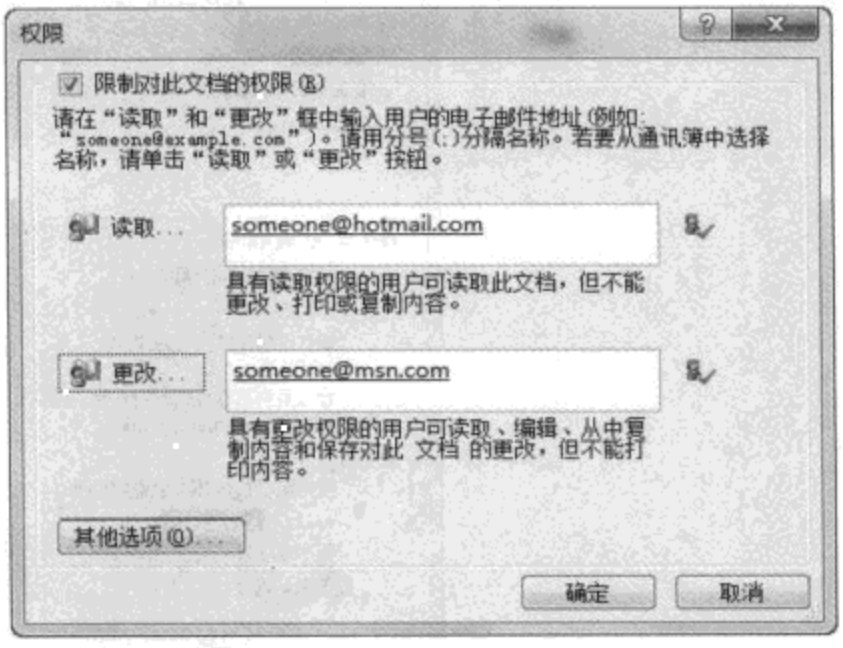


图 5-27　为文档的读者设置权限

首先，请选中“限制对此文档的权限”选项，随后可以在“读取”和“更改”文本框中指定可以读取该文档和更改该文档内容的用户。我们只需要把每个用户的 Windows Live 账户添加到对应的文本框中即可，同时可以使用半角分号（;）分隔多个账户，或者也可以单击“读取”和“更改”按钮，从自己的联系人中直接选择。

如果默认的这种权限设置无法满足要求，还可以单击“其他选项”按钮，进行更多的限制。单击该按钮后，可以看到如图 5-28 所示的“权限”对话框。在用户列表中已经列出了之前指定的用户的 Live ID，同时每个用户还会显示不同的访问级别。创建这个文档的人的访问级别是“完全控制”，输入到读取文本框中的用户的访问级别是“读取”，输入到更

改文本框中的用户的访问级别是“更改”。如果需要添加或者删除用户，请使用用户列表右侧的按钮。如果需要更改某个用户的访问级别，请将鼠标指针放置在该用户的访问级别上，程序会自动弹出一个下拉菜单，单击后即可选择不同的访问级别。

如果要共享的是有时效性的文档，只希望对方在某个日期之前才能打开，那么可以选中“此文档的到期日期为”选项，然后从下拉菜单选择一个到期日期。文档到期后将无法打开此文档。

如果打算允许用户打印该文档，可以选中“打印内容”选项，否则请反选。

IRM 保护有一个很明显的不足，如果希望文档在某个固定的日期过期，但对方如果希望过期后继续查看，完全可以在过期前将文档的内容复制出来。为了防止这种做法，可以反选“允许具有读取权限的用户复制内容”选项。当然，如果希望用户可以复制，则需要选中该选项。

如果文档中嵌入了宏，并且希望对方可以读取宏，就需要选中“以编程方式访问内容”，否则可以反选该选项。

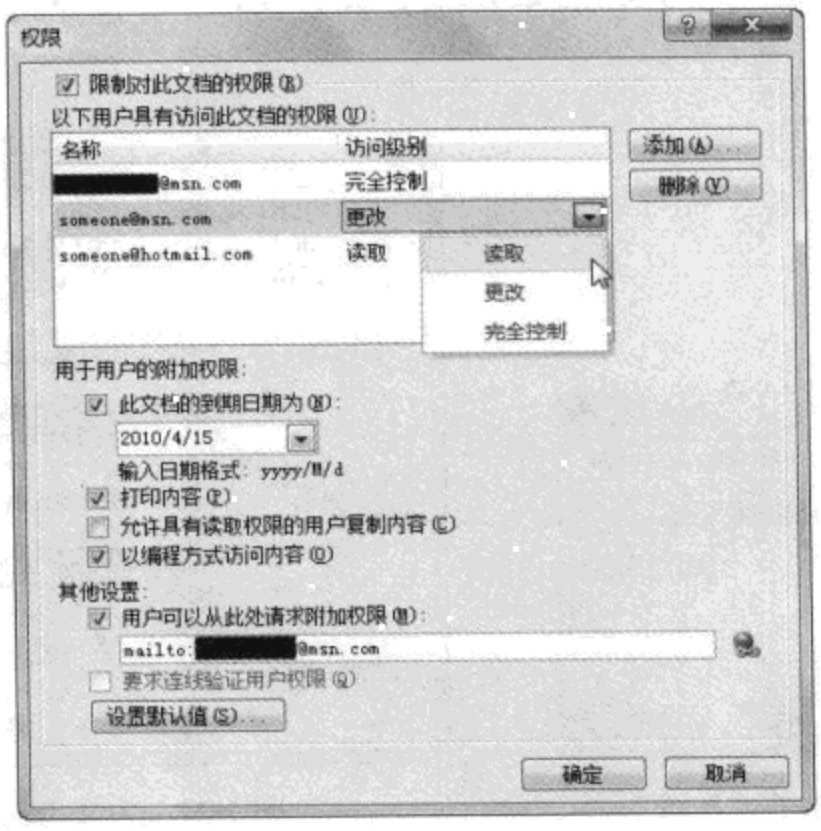


图 5-28　设置更详细的读者权限

如果希望别人可以向作者本人请求更多的权限，可以选中“用户可以从此处请求附加权限”选项。例如，使用 IRM 保护了一个文件，允许某人打开查看，但不允许对方编辑。如果对方确实需要编辑这个文件，可以用电子邮件联系我们，并索取相应的权限。当然，如果启用该功能，还需要提供可以联系我们以获取权限的途径，最常用的办法是使用电子邮件。

设置好之后，单击“确定”按钮即可。接下来，Word 窗口底部的状态栏上就会显示一个 IRM 图标，单击该图标后可以打开“权限”对话框调整权限设置。

5.5.2.2　查看 IRM 保护的文档

IRM 功能是从 Microsoft Office 2003 开始提供的，因此，这之后的 Office 版本才可以打开受 IRM 保护的文档。如果对方依然在使用更老版本的 Microsoft Office，或者希望使用 IRM 技术保护其他格式的文件，又该怎么办？

1．如果有支持 IRM 功能的 Office 软件

如果系统中安装的 Office 软件已经是支持 IRM 的新版本，则直接双击收到的文件即可。完整的过程如下：

STEP 01　对方收到我们的文件准备打开的时候，Office 首先会弹出一个对话框，询问是否立刻注册以获得凭据，单击“是”按钮。

STEP 02　随后会出现类似上文介绍的注册过程，请在该过程中使用自己的 Live ID 登录。注意，登录使用的 ID 必须是文档的作者在设置权限时指定的 ID。

STEP 03　在获取了个人证书后，Office 还需要联机验证我们所具有的权限，在这之前会询问是否允许联机验证，请选择“是”。

STEP 04　如果验证无误，文件可以直接打开，同时在 Office 软件窗口顶部会出现黄色的信息栏，告知该文档所受到的保护信息，窗口底部的状态栏会显示一个 IRM 图标，单击后可以打开一个窗口，查看自己当前登录的身份，以及可以进行的操作（如图 5-29 所示）。

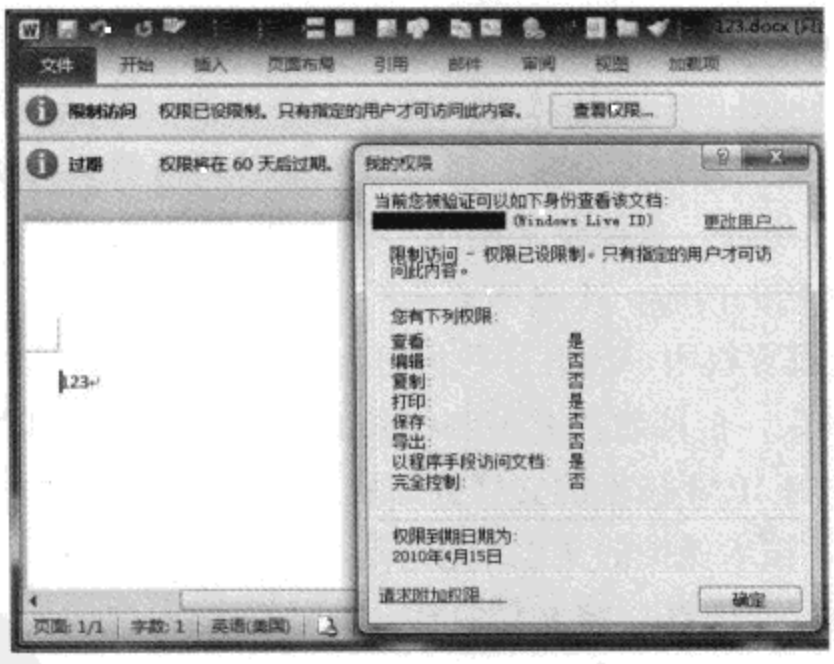


图 5-29　在高版本 Microsoft Office 中查看受 IRM 保护的文档

STEP 05　如果希望以其他用户的身份登录以查看该文档，请单击“更改用户”链接。

STEP 06　如果希望获得自己没有的权限，请单击“请求附加权限”链接，随后系统会自动调用默认的电子邮件客户端软件创建一封新邮件，并将文档作者留下的电子邮件地址输入到收件人一栏。

2. 如果没有支持 IRM 功能的 Office 软件，或者希望保护其他格式的文件

如果读者使用的 Microsoft Office 版本太老，或者作者希望使用 IRM 功能保护其他格式的文件，此时可以借助微软的 XPS 文档格式间接实现。

XPS 是微软开发的一种跨平台文档格式，该格式的用途与很多人熟知的 Adobe PDF 格式非常类似。要查看 XPS 格式的文档，首先需要安装 XPS 文档查看器（Windows Vista 以上版本的 Windows 系统已经内建该查看器，但仅限查看，无法创建）。这种格式可以实现在任何平台以及设备上，都能以完全一致的外观呈现文档内容，以及可以试试非常强大的权限保护等特点。

基本上，XPS 的相关特征也与 Adobe PDF 格式非常类似，只不过 PDF 格式的创建工具很多是需要付费的，虽然免费的 PDF 创建工具有很多，但 PDF 格式的保护功能仅限密码保护和数字证书保护。市面上有很多软件可以破除 PDF 文件的密码保护，数字证书保护虽然不易破解，但这样的数字证书和可支持使用证书提供保护的 PDF 创建工具往往都需要付费购买。比较而言，XPS 格式的相关工具都是微软免费提供的，因此，它更廉价、划算。要了解 XPS 格式的详细信息以及下载 Microsoft XPS Essentials Pack（包含 XPS 查看器和创建工具），请访问：http://tinyurl.com/yzalt5j。

在安装 Microsoft XPS Essentials Pack 后，安装程序还会给系统中安装一个名为 Microsoft XPS Document Writer 的虚拟打印机，该打印机的用途就是将任何可打印的文档都“打印”成 XPS 格式的文件。任何应用程序只要支持打印功能，就可以使用该虚拟打印机将文档转换为 XPS 格式。这样做有多种好处，例如，某台计算机上可能安装了一个非常昂贵的商业软件，该软件创建的文档格式是封闭的，必须使用这个软件才能打开和查看。如果希望将该软件创建的文档与别人分享，对方可能也必须付费购买软件。

有了 XPS 虚拟打印机后，只要将文档打印成 XPS 格式，对方安装免费的 XPS 查看器后，就可以直接看到文档的内容，不再需要购买昂贵的软件。另外在，打印 XPS 文档时，也可以使用 IRM 功能设置权限，因此，我们可以利用这一点，在高版本 Microsoft Office 软件中将需要分享给别人，但同时需要控制权限的文档打印成受 IRM 保护的 XPS 文档；或者也可以将其他不支持 IRM 技术的文档打印成 XPS，并传播给别人。

对于需要使用 IRM 技术保护的文档（无论是 Microsoft Office 文档，还是其他程序的文档），都可以像普通的打印那样，将文档打印出来。不过在打印时要选择 Microsoft XPS Document Writer 作为打印机（如图 5-30 所示）。取决于用于打印的程序，其打印对话框可能和这里列举的有所区别，不过大部分程序的打印功能都允许选择使用指定的打印机打印，并可提供按钮，用于对该打印机的参数进行设置。

单击“打印”按钮后，还需要指定打印出的 XPS 文件的保存位置。打印完毕后，在指定的位置找到并双击打开 XPS 文件，然后在 XPS 查看器的“权限”菜单下单击“设置权限”。

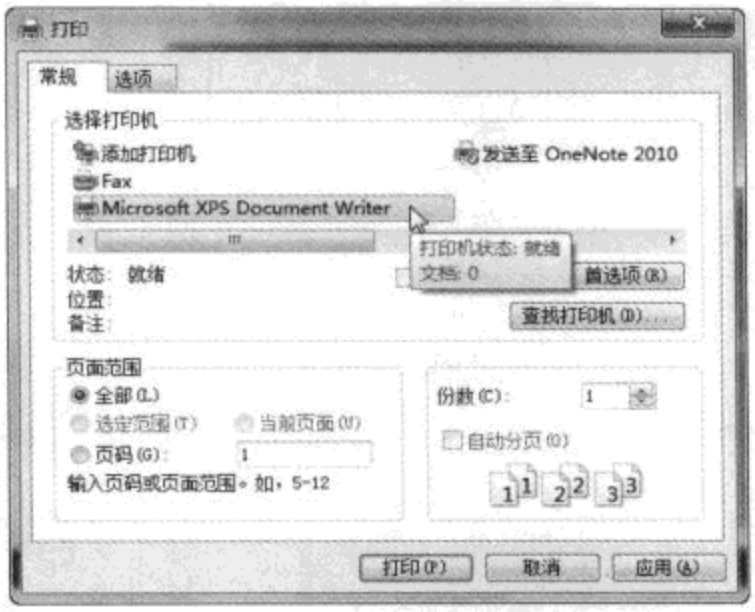


图 5-30　要选择正确的打印机

注意　凭据问题

虽然使用 XPS 文档格式可以获得受 IRM 保护的文档，但这并不意味着这种用法可以脱离 Microsoft Office 单独使用。要使用这一功能，一个核心要求是系统中必须包含 IRM 功能的相关凭据，在支持 IRM 的新版本 Microsoft Office 软件中，通过上文介绍的方法可以登录 Windows Live ID，并获得微软提供的凭据。然而，XPS 查看器本身并不能用于登录并获得凭据，这里还是需要借助 Microsoft Office 获得的凭据对 XPS 文档进行保护。不过，如果是部署了 IRM 架构的企业环境，则不受这一条件约束，就算不安装 Microsoft Office，也可以对打印出来的 XPS 设置 IRM 保护。

如果一切设置无误，随后将能看到图 5-31 所示的对话框。在这里，从 Microsoft Office 中获得的凭据对应的 Windows Live ID 将直接成为该文档的“作者”。随后，我们可以手工输入或者从联系人信息中选择等方式，将对方的 Windows Live ID 添加进来，并根据实际情况从右侧选择允许每个联系人获得的权限。这里的设置方法与上文介绍的 Office 中的方法基本上完全相同。

设置完毕后单击“保存”按钮，查看器会自动联网获取并提交相关的信息，此时会显示一个进度条，取决于实际网速，这个进度条可能会显示短暂时间。当进度条消失后，即可将 XPS 查看器关闭，并将获得的 XPS 文件发送给别人。

别人在收到这样的文件后，直接双击并调用 XPS 打开文件，随后将看到类似图 5-32 所示的对话框，此时必须单击按钮，使用文档作者指定的 Windows Live ID 登录，并下载必要的凭据信息，随后才能看到文档的内容，并获得文档作者在图 5-31。所示对话框中指定的权限。这个过程与使用 Microsoft Office 软件时获取凭据的过程完全相同，在此不再详细介绍。

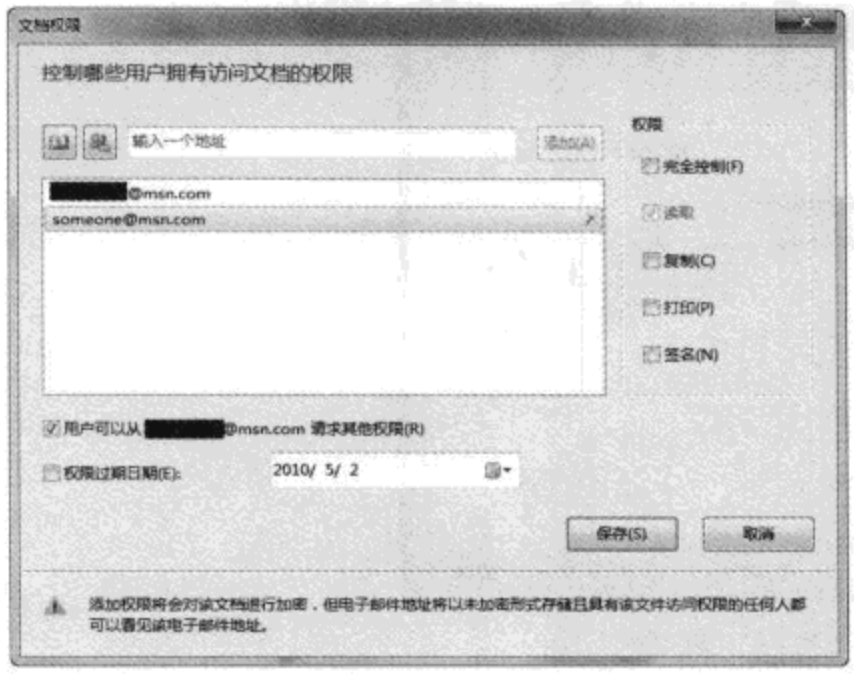


图 5-31　在 XPS 查看器中为文档应用 IRM 保护

图 5-32　受保护内容必须登录后才能看到

通过上文的介绍，相信大家已经对 IRM 有了一些基本了解。IRM 在保护文档方面确实有一些独到之处，但并不能仅仅依靠这些技术手段就觉得已经万无一失了。例如，如果我们限制对方只能在某个日期之前查看这个文档，并且禁止他打印和复制文档内容，那么对方完全可以在允许的时间内用截图软件对屏幕上显示的内容进行截取；如果我们通过软件限制策略限制了对方运行未经许可的软件，他还可以使用照相机或者摄像机把屏幕上的内容拍摄下来；如果我们制定规章制度，不准员工将照相机、摄像机甚至手机带入办公室，那他还可以用纸和笔将文件内容抄下来；如果禁止将纸笔带入办公室，那么对方还可以在允许查看的时候将文档内容背下来。

在这里说了这么多极端的情况，目的只是想告诉大家一件事：**只要将某个东西给别人看，那么信息泄露就是不可避免的**。

5.6　文件的彻底删除和反删除

当我们删除了一个文件，并且清空回收站后，这个文件真的就从硬盘上消失了吗？当我们无意中删除了本不该删除的文件后，还有没有办法挽回呢？

在讨论这个问题之前，我们首先回忆一下硬盘存储文件的原理，以及 Windows 删除文件的方式。大家都知道，对于一个新买的硬盘，如果打算在上面存储文件，首先必须给硬盘分区，并用某种文件系统将这个分区格式化，然后才能使用。在格式化的时候，格式化程序会将硬盘分区划分成大量的小块区域，这些区域叫做扇区。当我们在硬盘上保存文件的时候，文件首先被写入扇区中，然后有关该文件在硬盘上的位置信息会被保存到 MFT（主文件分配表）中。例如，MFT 中的信息会显示，在硬盘第几个分区的第几个扇区上保存有一个文件，文件的名字是什么，文件有多大，占用了几个扇区。

Windows 就是通过 MFT 中的这些信息判断文件是否存在的。而当删除某个文件的时候，为了能够快速删除，Windows 只是简单地将 MFT 中有关该文件的位置信息删除，实际上，文件的内容还保存在相应的扇区位置中。这样，如果向硬盘中写入新的文件，Windows 就会检索 MFT 信息，判断硬盘的哪些扇区是可用的（实际上，这些扇区中可能还有我们以前使用过的文件），并将新文件写入到该位置。

因此，如果一个文件被删除了，但保存这个文件的扇区还没有被覆盖新的数据的情况下，通过使用专门的反删除软件，完全可以将之前删除的文件重新找回来。

同理，如果需要彻底删除一个文件，不仅要删除 MFT 中的记录，还要删除硬盘扇区中实际保存的文件，我们也必须使用专门的软件给这个文件对应的硬盘扇区中写入垃圾信息，将其彻底覆盖，只有这样才算是完整的删除。

5.6.1　彻底粉碎文件

如果希望彻底擦除某个或某些文件，让文件无法通过恢复软件恢复，必须使用能够给硬盘上的扇区填充垃圾数据的专用软件。这类软件目前有很多，有需要付费的商业软件，也有可以免费试用的自由软件。通常，这类商业软件的功能比较丰富，而且其数据擦除效果可满足某些机构或部门的行业标准，因此，推荐在对数据安全性非常重视的环境下使用。作为普通用户，大部分免费的擦除软件已经可以满足要求。

下文将以微软的一个免费小工具 sdelete.exe 为例进行介绍。该工具需要在命令行下使用，但只需要一行简单的命令就可以将某一文件或文件夹彻底擦除，或者也可以将某一分区的所有可用空间内遗留的内容完全擦除。更难得的是，作为一个免费的工具，Sdelete 完全遵从美国国防部的 DOD 5220.22-M 标准，通常情况下，完全可以通过这个软件放心擦除敏感数据，而不需要担心可能导致的泄密。

要了解该工具的详细信息并下载它，可访问：http://tinyurl.com/28e5r3。

将 Sdelete 下载回来后，解压缩到合适的位置，即可在命令行下直接使用。该工具的使用语法和支持的参数如下：

```
sdelete [-p passes] [-s] [-q] <文件或目录>，或 sdelete [-p passes] [-z|-c] [分区盘符]
```

-c：将空闲空间用“0”填充。

-p passes：指定覆盖写入的次数。

-s：对子目录进行递归。

-q：擦除过程中不显示错误信息。

-z：清理空闲空间。

例如，如果希望将 C 盘根目录下名为“Folder”的文件夹连同其中保存的所有内容都擦除，并且覆盖写入 5 遍，可以使用下列命令：

```
sdelete -p 5 -s c:\folder
```

如果某个硬盘分区曾经保存过机密文件，但文件已经使用常规方法删除，随后希望确保使用反删除软件无法将被删除的文件恢复，则可以使用-z 参数清理空闲空间。通过使用该参数，sdelete 会对指定分区所有空闲的空间（也就是在分区的 MFT 中被标注为“可用”，但其中可能依然保留有机密数据的扇区）进行填充，为此可使用下列命令：

```
sdelete -p 5 -z d:\
```

注意，这个命令将对硬盘中所有空闲的空间进行填充，并且可以通过-p 参数指定填充的次数。因此，如果目标分区的容量比较大，或者指定了较多的覆盖次数，整个过程将耗费很长时间。

> **提示**
>
> 对于保密要求比较严格的场合，无论使用本书介绍的 Sdelete 还是其他商业化的数据擦除工具，都建议反复擦除多次。因为传统硬盘所具有的剩磁效应可能会导致擦除一两次后，依然存在数据被高精度机器恢复出来的可能性。因此，建议根据实际情况考虑数据的擦除方法。对于普通人涉及隐私的内容，例如数码相机的存储卡，或者退役电脑的硬盘，通常只要使用市面上可以获得的擦除软件反复擦除多次，就可以获得满意的效果。如果是要求非常严格的场合，还可以考虑通过物理或化学方式将硬盘的整个硬件彻底破坏。不过在进行这样的破坏时一定要确保做得足够彻底，因为根据报道，美国 2003 年爆炸的哥伦比亚号航天飞机上找回的一块硬盘，经过长达五年时间的处理后，其中的数据有 99%被恢复了出来（http://tinyurl.com/ya4a9v6）。

5.6.2 恢复被误删除的文件

介绍过怎样将文件彻底删除后，下面介绍怎样恢复被误删除的文件。市面上有很多收费不菲的数据恢复公司，可对各种情况下的文件丢失进行数据恢复。不过，如果文件的丢失只是因为误操作导致的，硬盘本身没有硬件故障，那么通过使用合适的软件，完全可以自己恢复丢失的数据。因为对于这种恢复，数据恢复公司采用的也是类似的方法。

注意，本节介绍的方法仅适合在 Windows 中使用常规方法删除并清空回收站的文件，并不适合使用上一节介绍的软件擦除导致的“删除”，软件覆盖擦除这种操作在理论上是不可逆的，一旦被覆盖，就永远无法恢复。

在恢复被误删除的文件之前还有一点需要注意：一旦发现自己误删除了重要文件，请在第一时间立刻关掉计算机（直接拔电源，而不是从“开始”菜单中关闭）。然后将被删除文件所在硬盘拆下来，连接到其他计算机上（这台计算机最好暂时禁止任何可能需要给硬盘进行写操作的程序，例如后台的杀毒软件、磁盘碎片整理工具、索引工具等），使用反删除软件进行恢复。这样做的主要目的在于尽量避免有新的数据被写入硬盘，而无意中覆盖了误删除文件占据的硬盘扇区。毕竟 Windows 在将文件写入硬盘的时候是随机的，新文件

可能被写入硬盘上任何一块可用的扇区中，而一旦被误删除的文件所在的扇区被新文件覆盖了，那么该文件可能无法被恢复，或者恢复出来的数据不够完整。因此，为了提高恢复的成功率，在误删除后，请一定不要再使用这块硬盘。

市面上有很多反删除软件，其中有些是收费的商业软件，有些则是免费的自由软件。很多人从上文介绍的原理中已经意识到了，这类软件的工作原理也是非常类似的：绕过 MFT 直接扫描硬盘指定位置的每个扇区，然后从中找出所有可恢复的数据，并供我们有选择地恢复。

严格来说，收费的商业软件和免费的自由软件在实际效果上的区别并不大。不过有些收费软件的功能更全面，例如某些反删除软件是专门针对某一类型的文件提供恢复的；有些收费软件则提供更全面的筛选功能，可通过指定要恢复的文件的名称关键字、大小、创建时间等参数，加快文件的扫描和恢复速度。大家可以根据实际需要选择要使用的软件。而且取决于具体的软件算法和实现方式，有时候可能一个软件无法恢复的文件可以通过另一个软件顺利恢复。在实际使用中，也可以结合具体情况选择软件。

> **注意**　卷影副本功能
>
> 除了使用反删除软件恢复被误删除的文件外，还可以使用 Windows 7 自带的卷影副本功能帮助保护重要的内容。通过使用卷影副本，可以随时将某个文件或文件夹恢复到之前的某一状态下。有关该功能的详细介绍，请参考本书第 13 章有关卷影副本的介绍。

在选择反删除软件时需要注意，很多收费的商业软件往往还会提供试用版，取决于不同的软件，试用版可能存在不同的限制。例如，有些软件的试用版可供我们扫描整个硬盘，找出所有可恢复的文件，如果发现其中有需要的文件，则需要付费购买，然后才能恢复。有些软件则可能是在付费购买前，只能恢复体积不超过某个预定值的文件。有些软件则可能会提供有限天数的全功能使用，对于这类软件，自然是最适合我们的，因为完全可以在有限的试用期内找到并恢复重要的文件。

下文将以一款免费的软件 Recuva（http://tinyurl.com/c3eosk）为例进行介绍，这个软件完全免费，没有任何功能限制，而且具有中文界面（虽然有中文界面，但汉化不够全面，有些选项依然是英文的，但该软件的使用并不难）。因此，更适合普通用户（注意，在撰写本书时，该工具的 1.36 版安装文件捆绑有工具栏，安装过程中是被默认选中的，但可以反选，因此，不需要工具栏的读者需要反选该选项，即不安装）。使用该软件恢复误删除文件的步骤如下：

STEP 01　在其他计算机上安装该软件，然后将误删除文件所在的硬盘连接到这台计算机上（如果硬盘类型不匹配，例如，误删除的文件在台式机上，另一台计算机是笔记本，则可以使用外置硬盘盒安装硬盘，然后用 USB 接口将其连接到笔记本进行恢复）。

STEP 02　启动 Recuva，默认情况下，该软件运行时会显示一个向导，通过回答向导提

出的问题，可以缩小文件的排查范围，加快文件的扫描和恢复速度。在向导的第一个页面上单击“下一步”按钮。

STEP 03 随后可以看到图 5-33 所示的界面，在这里首先要选择待恢复文件的类型。因为不同类型的文件具有不同的特征，因此，如果能明确指定文件类型，恢复软件的扫描和恢复速度都可以更快一些。在这里请根据实际情况选择，或者选择“Other”，不考虑文件类型的差异。

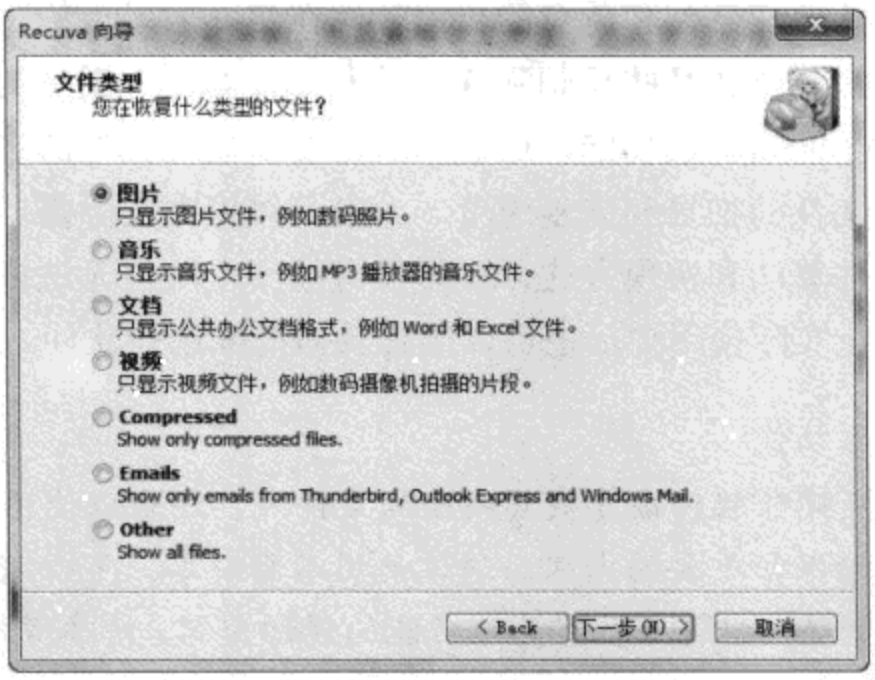


图 5-33　选择要恢复的文件类型

STEP 04 随后需要在图 5-34 所示的界面上选择文件的位置。注意，因为反删除软件需要对硬盘上的位置进行逐扇区地扫描，而现在的硬盘往往都很大，因此，扫描过程通常需要很长时间。如果能指定一个扫描范围，例如某个分区，或者某个文件夹，扫描的过程将会短得多。

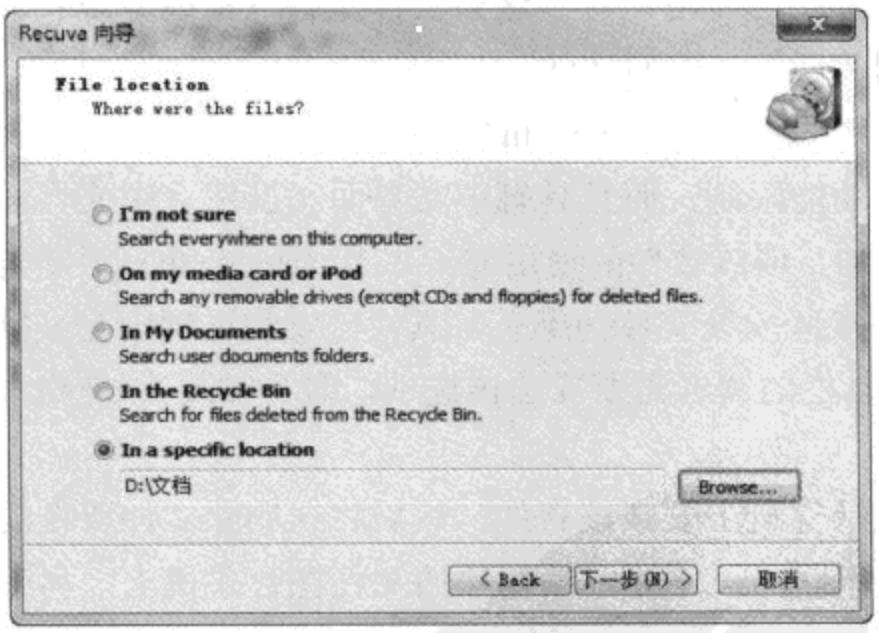


图 5-34　选择文件的大致位置

在这里可用的位置选项包括：

- **I'm not sure（不确定）**　如果忘记了文件之前保存在哪里，或者想知道自己的整个硬盘上都能恢复出多少文件，可以使用该选项，但扫描速度是最慢的。
- **On my media card or iPod（在我的存储卡或 iPod 上）**　如果要恢复的文件位于存储卡，或其他可移动存储设备，或者可被计算机识别为存储设备的其他设备，例如数码相机、便携式播放器等，可以选择该选项。
- **In My Documents（在我的文档文件夹中）**　如果要恢复的文件位于默认的“文档”文件夹，可以选择该选项。
- **In the Recycle Bin（在回收站中）**　如果文件之前曾经在回收站中，但清空了回收站，可以选择该选项。
- **In a specific location（在指定的位置下）**　如果需要手工指定扫描的目录或位置，可以使用该选项，并指定位置。

STEP 05　随后可以通过选项启用深度搜索，该选项的扫描更加彻底，但也更慢。因此，建议首先不选择该选项，只有在扫描后发现需要的文件并未找到时再考虑使用。准备好后单击“开始”按钮。

STEP 06　取决于之前选择的内容，整个扫描过程可能会需要几秒钟、数分钟，甚至数小时，请耐心等待。扫描结束后，可以看到图 5-35 所示的界面。

STEP 07　所有扫描到的文件都会直接列在窗口中，其中带有绿色圆圈的文件意味着是可以正确恢复的，红色圆圈标注的文件都是无法恢复的。对于无法恢复的文件，在“注释”一栏可以看到相关的原因，例如本例中，无法恢复的文件都是因为有扇区被其他文件覆盖导致的。对于可恢复的文件，只要选中对应的复选框，然后单击右下角的“恢复”按钮即可。注意，在保存恢复出的文件时，一定不能选择该文件所在的硬盘或分区，必须将其保存到其他位置。

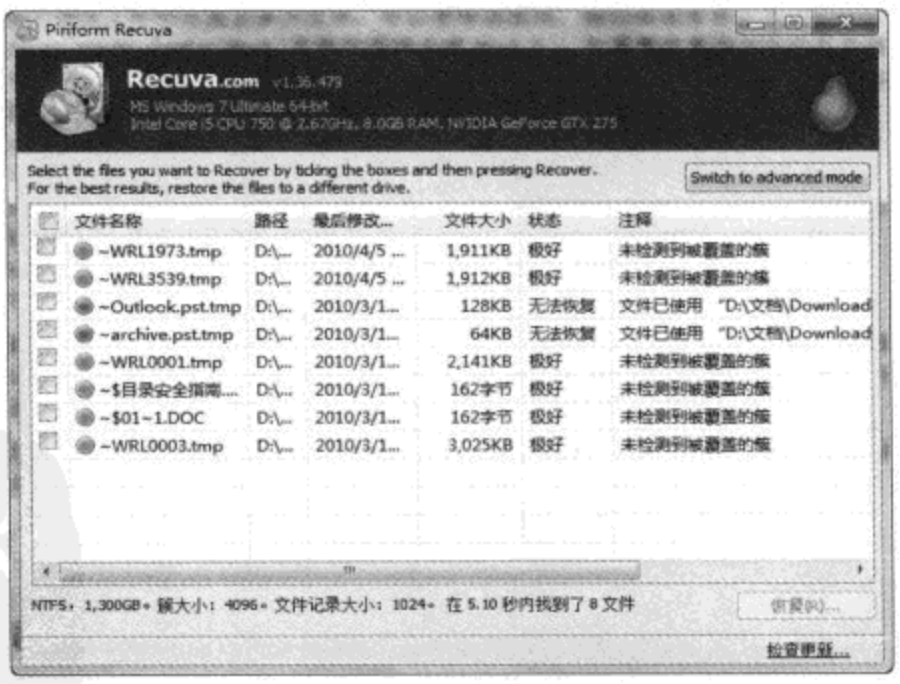


图 5-35　扫描后的结果

作为一个免费的软件，Recuva 的功能相当强大，在图 5-35 所示的界面右上角单击“Switch to advanced mode（切换到高级模式）”后，还可以在高级模式下对扫描到的结果进行关键字搜索和排除，并且可以预览文件的内容或文件头信息，这些功能都有助于更准确地找到想要恢复的内容。

另外，该软件也带有文件覆盖擦除功能。对于不需要保留的内容，只要鼠标右键单击它，并选择相应的“安全覆盖”选项，程序就可以对文件位置重复填充随机数据，将其彻底擦除。

2

第 2 部分
网络安全

现在的计算机安全环境已经不再像以前那样单一了，因为网络的使用得到了大范围的普及。在以前的单机时代，一台计算机上有病毒或者有漏洞，影响的范围可能很小。而现在，如果有感染病毒的计算机接入网络，可能在很短的时间里就能感染大量计算机，造成很严重的后果。至于互联网，因为以前人们的互联网连接速度普遍不快，因此，通过网络传播的病毒或者恶意程序的传播速度很慢，而且很容易被发现。现在的高速互联网连接随处可见，病毒可能会在我们毫无知觉的情况下感染自己的计算机，并继续向其他计算机传播。

另外，各种恶意软件的层出不穷也开始令很多人闻之色变。在以前，恶意软件（主要是计算机病毒和木马）的编写纯粹可以理解为一种“炫技”，这类软件的作者希望通过编写一些恶作剧程序获得别人对自己技术的认可。现在，此类软件大部分都是为了牟利而生的，一旦感染，可能会导致不小的损失。

因此，在保证操作系统本身安全的前提下，我们还应该尽可能地保证自己的网络安全。

本部分主要讨论网络的安全问题，例如无线局域网的安全，以及传统的有线局域网的一些设置。不仅如此，我们还将了解到怎样通过网络防火墙将网络攻击拒之门外。

CHAPTER

6

第 6 章　无线网络安全

无线网络的普及速度很快。基本上，只要能够通过无线的方式用电磁波传输数据的网络，都可以叫做无线网络，例如，最常用的基于 IEEE 802.11 协议及其各种变体的 WiFi 无线网络、使用蓝牙技术在小范围内传输数据的蓝牙网络、使用 GPRS/EDGE/CDMA 等技术借助无线通信运营商网络传输数据的广域无线网络等。本章主要关注基于 802.11 协议及其变体的 WiFi 无线局域网。

对于 WiFi 网络，随着 Intel 公司迅驰技术的普及，它已经深入人心。任何人只要有安装了兼容的 WiFi 网卡的计算机，并且能够找到提供 WiFi 服务的无线基站，就可以接入到 WiFi 网络中，实现各种便捷的功能。和传统的有线网络相比，WiFi 最大的优势在于无线，因为我们不需要再拖着长长的网线访问网络，只要在无线基站电磁波的覆盖范围内，我们就可以随时在移动中访问网络。然而这种无线的访问方式也正是 WiFi 网络在安全上的最大不足。

在传统的有线网络中，如果别人要访问我们的网络，必须用网线将自己的计算机和网络设备连接在一起。这本身就是不容易做到的事情，毕竟没有哪个公司会允许一个陌生人将自己的计算机连接到公司的交换机上，而且我们可以通过追踪网线的方法找到每一台连接到网络中的计算机的具体位置。然而在 WiFi 无线网络中，这一切就变得困难了，毕竟少了网线，任何人只要能够接触到足够近的位置，就可以借助电磁波连接到别人的网络，同时，如果没有专业设备和专业知识的帮助，想要判断无线连接的计算机的位置，基本上是不可能的。

其实，IEEE 工作组在制定 WiFi 网络的技术标准时，就已经考虑到了这些问题，并制定了有效的措施防范这类问题给我们的网络带来任何危险。只不过，很多人因为不了解这些内容，或者不够重视，才会让自己的 WiFi 网络暴露在危险中。

本章将介绍一些常见的 WiFi 网络标准，这些标准的优点和不足，以及如何利用现有的技术提高自己无线网络的安全性。

> **注意**　WiFi 网络的称呼
>
> 在称呼“使用 802.11 协议及其变体协议的无线以太网”的时候，很多人习惯将

> 其称为 WiFi 网络，其实这是一种不够严谨的说法。WiFi（Wireless Fidelity）是无线局域网联盟（WLANA）的商标，该商标与无线网络使用哪种标准没有太大关系。但因为很多人已经习惯了这种称呼，因此，本书也打算将使用各种 802.11 协议的无线以太网叫做 WiFi 网络。

WiFi 网络可以工作在两种不同的模式下：自由直连（ad hoc）以及基站访问（Base Station），其中，自由直连的方式类似于有线网络中的双机互联，可以由多个无线设备在不借助中央网络设备的情况下组成一个临时性或者永久性的无线网络。而基站访问类似传统有线网络中的星形网络，必须有一个中央网络设备，这个设备叫做无线基站，起到了提供无线信号、交换机、路由器或者集线器的作用。通常来说，我们最常用的模式都是基站访问，因此，本书也重点介绍基站访问模式下的 WiFi 网络安全。

在基站访问模式下，需要有无线基站参与其中，因此，整个 WiFi 网络的安全性主要取决于无线基站的设置，因为每种品牌和型号的无线基站的具体设置方式不同，本书将以巴比禄（Buffalo）WZR-HP-G300NH 802.11n 无线路由器为例进行介绍。无线基站的设置基本上都需要使用网页浏览器访问无线基站的 IP 地址，然后在浏览器中进行配置，在这之前必须使用有效的用户名和密码登录。关于无线基站的配置页面 IP 地址，以及默认的用户名和密码，请参考设备说明书。

6.1　常见的无线网络标准

目前，我们能够接触到的 WiFi 无线网络基本上都使用了 IEEE 802.11 标准，这个标准很早以前就诞生了，并且随着时间的延续和用户要求的变化产生了大量不同的变体，常见的变体包括 802.11、802.11a、802.11b、802.11g，以及 802.11n。这些标准都有什么特点，应该怎样选择？

802.11 是 WiFi 网络的第一个标准，诞生于 1997 年。该标准使用了 2.4GHz 频率的无线电波，最大的数据传输速率为 2Mb/s，室外的有效传输距离可以达到 75m 左右。这种标准最大的不足在于传输速率，同时该标准的安全性也很有限。

1999 年，IEEE 工作组发布了 802.11a 标准，这是对 802.11 标准的改进，这种新的标准使用了 5GHz 频率的无线电波，最大的数据传输速率为 54Mb/s，室外的有效传输距离可达 75m。因为该标准使用的 5GHz 频率在很多国家的使用受到限制，因此，该标准一经发布，很快就被 802.11b 标准取代。

同样在 1999 年，802.11b 标准也发布了，该标准依然使用最容易被接受的 2.4GHz 频率的无线电波，最大的数据传输速率为 11Mb/s，室外传输距离可达 100m。该标准曾经是使用率最广泛的 WiFi 网络标准，不过因为数据传输速度太慢，逐渐开始被 802.11g 标准取代。

802.11g 标准诞生于 2003 年，该标准使用 2.4GHz 频率的无线电波，最大的数据传输速

率可以达到 54Mb/s，室外的有效传输距离可以达到 100m 左右。目前我们使用最多的绝大部分 WiFi 网络都是用了该标准。

虽然 802.11g 标准很普及，但该标准的数据传输速率相对传统的有线网络还是低很多。因此，IEEE 工作组目前已经正式发布了新一代的标准 802.11n，虽然该标准目前已正式发布，但由于其草案经历了较长的讨论阶段，因此，市面上使用该标准的产品大部分都是兼容 802.11n 草案的产品，完全符合正式标准的产品还不多。该标准可以使用 2.4GHz 或者 5GHz 频率的无线电波（有些产品为了提高抗干扰能力，可同时使用这两个波段），最大的数据传输速率可以达到 300 Mb/s，室外传输距离可达 160m 左右。

根据实际情况来看，目前 WiFi 网络使用最多的标准依然是 802.11g/n，同时支持这些标准的设备都是互相兼容的，这就类似以前我们常见的十兆/百兆自适应网卡，在十兆网络中就工作在十兆模式下，在百兆网络中就工作在百兆模式下，一般的 WiFi 网卡也可以根据网络的实际情况选择不同的标准来使用。

如果希望决定无线基站使用的标准，请登录到无线路由器的设置页面，找到有关无线网络的设置，并寻找“协议”、“标准”或“模式”之类的选项，一般情况下，如果无线路由器可以使用不同的标准，那么相应的标准就会显示为选项供我们选择。

通常，在设置无线路由器的工作模式时，需要照顾到最低模式的设备。例如，很多无线路由器已经同时支持 802.11b/g/n 模式，并可在这些模式之间切换，但如果有只能支持 802.11b 模式的设备需要通过该路由器访问网络，那么路由器就必须提供 802.11b 模式的选项。如果所有的设备都支持较新的标准，就尽量选择新的标准，毕竟新标准不仅速度更快，而且更加安全。

6.2 加密方式的选择

在上文中曾经说过，WiFi 网络最大的优点和不足都是“无线”。因为无线，所以使用更加方便；也正是因为无线，网络会暴露给所有处于无线电波覆盖范围内的人。在无线网络中，任何可以访问到网络的人使用嗅探器之类的软件，就可以截获网络中传输的数据，造成泄密或者更加严重的安全问题。

为了避免出现这种状况，WiFi 网络的通信可以进行加密。这样就算别人截获了数据，因为无法解密，也无法获知其中的内容。经过多年的发展，WiFi 网络可用的加密方式有很多，一般来说，比较常见的加密方式按照其出现的先后顺序以及安全性来看，主要有 WEP、WPA 和 WPA2。

WEP（Wired Equivalent Privacy，有线等效加密）是早期很常用的一种加密方式，在使用这种加密方式的情况下，网络通信会被使用 40 位或 104 位的密钥进行加密，一般较老的设备可能依然在使用这种加密方式。因为在 WEP 方式中，网络上的所有设备共享使用同一个密钥，同时该密钥存在不安全的因素，因此，WEP 的安全性现在已经变得相当差，并且

很容易被破解，网上甚至有很多工具软件可以用于破解 WEP。因此，如果设备还支持其他加密方式，强烈建议不要继续使用 WEP。如果设备尚不支持其他加密方式，请尝试升级设备的固件，因为某些设备在升级固件后可能会增加其他加密方式。如果设备通过升级也无法支持其他加密方式，同时又比较注重安全性，那么可以考虑更换设备。

WPA（Wi-Fi Protected Access，WiFi 保护访问）是一种较新的加密方式，在使用这种加密方式的情况下，网络通信会被使用 TKIP（Temporal Key Integrity Protocol，临时密钥集成协议）密钥加密，同时每个网络设备都将使用不同的密钥。因此，相比 WEP，WPA 更加安全，在此推荐采用。

WPA2 是 WPA 的改进版，主要改进之处在于 WPA2 使用了新的身份验证和密钥管理机制，并使用了更加高级的加密标准。因此，在目前的常见设备中，WPA2 加密方式相对来说是最安全的。

在选择无线路由器使用的加密方式前，请首先根据说明书中的介绍升级路由器的固件，因为新版本的固件可能会提供新的加密方式。升级固件到最新版后，打开无线路由器的配置页面，找到和“无线安全”有关的选项，如图 6-1 所示。

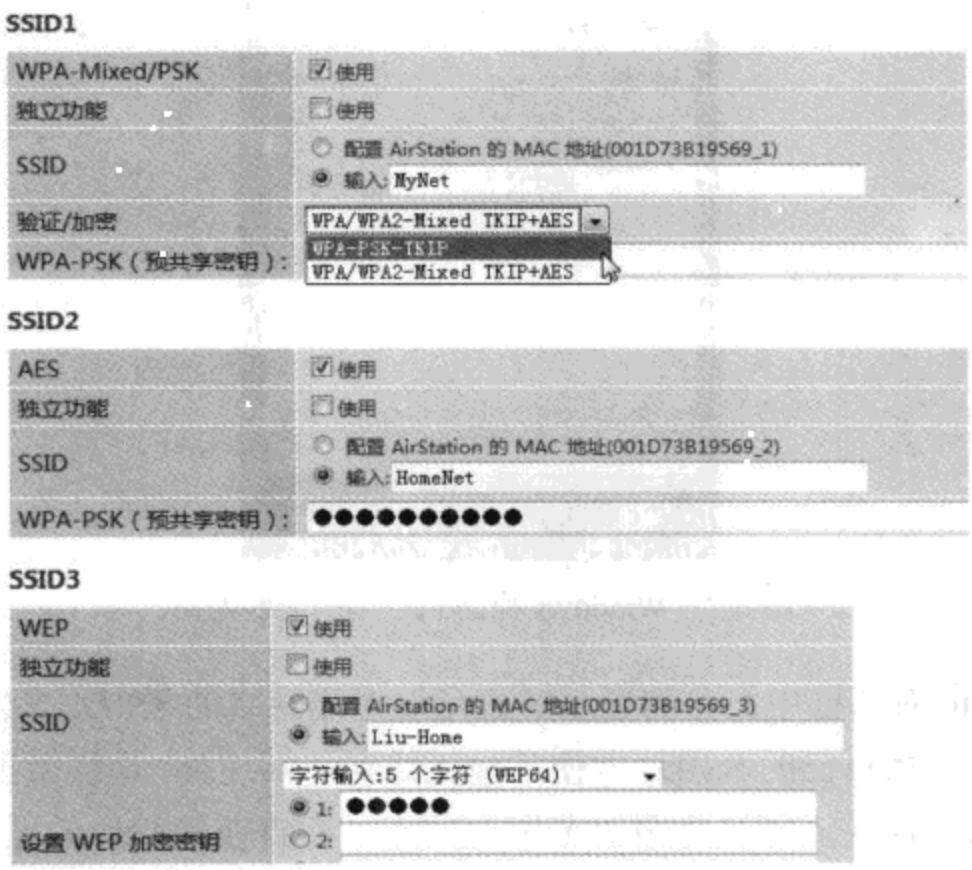


图 6-1　对不同的 SSID，选择要使用的加密方式

在图 6-1 中，应该根据设备的支持情况选择最安全的加密方式。例如，如果可以支持 WPA，就不要选择 WEP；如果支持 WPA2，就不要选择 WPA。选择好后还需要根据选择的加密方式输入不同的密钥。请在加密方式允许的前提下尽量使用较长、较复杂的密钥。

有些比较新的路由器可支持多 SSID 功能，也就是说，虽然只有一个无线设备，但可以表现为多个不同的独立无线网络，每个网络有自己的 SSID 和安全设置。因此，如果可

能，也可以使用这样的功能，并根据不同的无线模式和安全标准对网络进行区分。这样高速新设备可以访问高速网络，低速老设备可以访问低速网络。这些不同的网络之间可以互通，也可以互相隔离，通常提供多 SSID 功能的路由器都会有类似的控制选项。

6.3 SSID

SSID（Service Set Identifier，服务匹配标识符）可以理解为无线网络的名称。当启用了计算机上的无线网卡后，无线网卡就会不停地扫描周围空间内的无线网络信号，如果找到了无线网络信号，就会通知我们，并尝试连接。计算机上的无线网卡是通过无线网络的 SSID 来判断无线网络的存在的，同时，我们也需要通过 SSID 区分不同的无线网络。例如在 Windows 7 中，在打算连接到无线网络的时候，如果系统检测到无线网络的存在，就会显示在图 6-2 所示的界面中。

图 6-2　Windows 检测到可用的无线网络

在图 6-1 显示的对话框中，左侧显示的就是该无线网络的 SSID。默认情况下，无线路由器都会向空间中广播自己的 SSID，方便其他无线客户端连接，这样做虽然提高了易用性，但并不安全，因为任何在无线信号覆盖范围内的人，都将获知我们的无线网络的名称，这容易造成两个问题：

- 别人在知道我们的无线网络 SSID 后，可以尝试连接，虽然在没有密码或者无线网络过滤 MAC 地址的情况下无法成功连接，但这至少存在一定的安全隐患。
- 很多无线路由器的设置中，默认情况下会使用无线路由器的制造商名称或者具体型号作为 SSID，在使用这样的默认设置下，任何人都将知道我们的无线路由器的品牌或型号。而一旦使用的产品存在某些已知或未知的漏洞，别人将很容易破解（要知道，就算不连接到某个无线网络，也很容易得知某个无线网络的 SSID）。因此，也

建议更改默认的 SSID，这样别人至少无法通过 SSID 判断无线路由器的型号。

在 SSID 方面，建议设置让路由器不广播自己的 SSID。在这种情况下，任何人在查找可用无线网络的时候都将无法找到我们的网络，但只要是知道 SSID 的人，就可以直接输入网络的 SSID 进行连接。毕竟在不广播 SSID 的情况下，WiFi 网络也是存在的，并且处于工作状态下。

通常，这类选项都位于“高级无线设置”之类的页面下，选项的名称应该类似于“启用 SSID 广播”，对于这种选项，请反选。当然，如果无线路由器提供的选项名称叫做“禁用 SSID 广播”，应该将其选中。

另外，如果无线网络必须广播 SSID，也建议至少将其改成使用非默认名称。通常，SSID 的名称是由“网络名称”之类的选项决定的。

6.4　MAC 地址过滤

虽然可以使用不同的加密方式对无线网络的通信进行加密，但这依然存在一个问题，只要是知道 SSID 或者网络密码的人，就可以通过无线的方式连接到我们的无线网络。这依然显得不够安全，毕竟我们还没能“硬性”决定谁可以加入到无线网络。

很多无线路由器都提供 MAC 地址过滤的功能，MAC 地址是网卡上的一串字符，简单地说，可以理解为网卡的身份证，无论是有线网卡还是无线网卡，都有全球唯一的一个 MAC 地址。因此，可以通过设置，只允许特定 MAC 地址的网卡连接到无线路由器。

首先需要知道自己无线网卡的 MAC 地址，在 Windows 中运行 cmd，打开命令提示符窗口，然后输入“ipconfig /all”命令，并按下回车键，这样，本机安装的所有网卡的硬件信息都会被列出来，请记下如图 6-3 显示的无线网卡的 MAC 地址。

```
无线局域网适配器 无线网络连接:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . . . . . . . . . . : Broadcom 802.11g 网络适配器
   物理地址. . . . . . . . . . . . : 00-90-4B-6B-DB-7E
   DHCP 已启用 . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . : fe80::ad25:1708:28c:c0df%9(首选)
   IPv4 地址 . . . . . . . . . . . : 192.168.1.252(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . : 192.168.1.1
   DNS 服务器 . . . . . . . . . . . : 208.67.222.222
                                       208.67.220.220
   TCPIP 上的 NetBIOS . . . . . . . : 已启用

以太网适配器 Local Area Connection:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . . . . . . . . . . : Microsoft Windows Mobile Remote Adapter
   物理地址. . . . . . . . . . . . : 00-02-B3-92-A8-C4
   DHCP 已启用 . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . : 是
   IPv4 地址 . . . . . . . . . . . : 169.254.2.2(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
```

图 6-3　查看无线网卡的 MAC 地址

请留意图 6-3 显示的结果，对于 Broadcom 802.11g 网卡，其“物理地址”一栏显示的就是该网卡的 MAC 地址，可将网卡的 MAC 地址记录下来备用。

随后登录无线路由器的配置页面，找到“MAC 地址过滤”或者“无线访问控制”之类的选项，将之前记录下来的 MAC 地址输入，并设置为“允许”即可。同时，为了方便日后的管理，有些路由器还允许我们为每个不同的 MAC 地址指定一个设备名，这样通过设备名就可以知道这是哪个设备的地址（如图 6-4 所示）。

图 6-4　通过 MAC 地址对无线网络的访问进行限制

经过上述设置，只有在无线路由器中指定过的 MAC 地址的网卡才被允许连接到这个无线网络，这无疑提高了安全性。同时，只要保管好无线路由器配置账户的密码，别人就无法修改设置。

在使用该功能的时候需要注意，很多无线路由器在提供了无线功能的同时，还提供了有线以太网接口，供没有无线网卡的计算机通过网线连接。对于有些无线路由器，通过有线网络连接的设备不会受到 MAC 地址过滤功能的影响，就算没有允许有线网卡的 MAC 地址，这些网卡依然可以连接进来。但有些无线路由器，MAC 地址过滤功能还会影响到有线网卡，对于这类设备，如果发现有线网卡无法连接进来的时候，请试试看将有线网卡的 MAC 地址也添加进来。

6.5　其他注意事项

WiFi 网络安全方面需要注意的问题就是上述这些内容。但是对于无线路由器本身，我们还有一些问题需要注意，下文将分别说明。

1. 管理员的密码

可以说，在基站访问模式的 WiFi 网络中，整个网络的安全性取决于无线路由器的设置。哪怕无线路由器提供很安全的功能，如果没有设置好，可能都会功亏一篑。因此，一定要保证别人无法随意修改我们的路由器设置。

对于绝大部分通过 Web 页面配置的无线路由器，在访问配置页面的时候，都需要输入正确的用户名和密码。这些设备在出厂的时候使用了默认的用户名和密码，在开始使用这台无线路由器的时候，一定要修改默认的用户名和密码，这是保证安全的基础。

当然，各种无线路由器的具体情况不同，有些只允许修改管理员账户的默认密码，但不允许修改用户名。因此，如果设备允许，最好修改默认的用户名。同时，管理员的密码最好使用一个和无线网络中所有计算机上的账户密码都不一样的密码。

2．远程管理功能

为了方便使用，很多无线路由器提供了远程管理功能。在启用这种功能的情况下，我们在地球上任何一个角落都可以通过互联网访问到无线路由器的 Web 页面，并对路由器的设置进行调整。

这种功能本来是为了方便使用而设置的，然而该功能带来的安全隐患远远超过了提供的便利。因此，如果不是有特殊需要，强烈建议关闭这种功能。毕竟对于大部分人，无线路由器只要配置好了，就可以直接使用，没必要频繁地调整其设置。

同时，有些路由器还有类似这样的限制：只允许通过网线连接的客户端对路由器的设置进行修改，而不允许通过无线网络连接的用户修改设置。对于有这种功能的路由器，也建议启用该功能。

3．理性对待 DHCP 服务

目前的绝大多数无线路由器都带有 DHCP 服务，可以为连接到网络的客户端自动分配 IP 地址，以及其他网络设置。这种功能对于某些场合是很有用的，例如，提供无线上网服务的咖啡馆或者机场，因为在这种环境下，流动用户很多，与其让每个流动用户都需要向管理员询问正确的网络配置参数，不如通过 DHCP 功能让无线路由器自行配置。

然而，这种功能在家庭环境下基本上没什么用处，因为我们对自己网络的所有配置参数都很了解，同时，家庭环境下很少会有新的设备加入进来。本着“最少的服务等于最大的安全”这一原则，如果不需要 DHCP 功能，请将其禁用。

4．公用热点是否可靠

现在很多地方都部署了无线路由器，并且很多都是公开的。例如，在会展中心或者机场等公共场所，往往都有不需要登录的无线网络供我们使用。任何人只要在信号覆盖范围内，搜索到这样的网络后就可以直接连接，并用于访问互联网。

这种在公共场所提供了无线网络服务的地方就叫做“热点”。和私有无线网络不同，在私有无线网络中，我们需要严格禁止外人连接，因此，往往会采取各种限制措施。而对于这种公用的热点，其本意就是为了给公众提供服务，因此，不仅不会进行任何限制，往往还鼓励大家使用。

公用热点的出现在给我们带来便利的同时，也带来了不小的风险，主要体现在隐私的

泄露和局域网安全方面。

首先，如果连接到公用热点，上网看看新闻当然没问题，毕竟没人会过于注意一个普通人到底是关心国内新闻还是国际新闻。但如果打算通过公用热点收发邮件或者进行网络交易，就要仔细掂量一下了。如果连接的热点恰好是某个别有用心的人专门设立的（这种情况目前虽然少，但依然存在），这些人往往会对通过该热点传输的数据进行窃听，并从中收集有价值的信息加以利用。虽然在收发邮件或者网络交易的时候有其他措施保护我们的信息安全（例如，SSL 加密或者数字证书），但同样存在安全隐患。

另外，在连接到公用热点后，我们和其他所有连接到该热点的人等于同时加入了一个大的无线局域网中。虽然有些热点通过一定的安全设置会自动隔离所有的用户，但如果设置错误或者某个热点没有提供这种功能，这依然会对我们的计算机安全造成威胁。例如，他人可能会访问到我们的共享文件。

在这方面，Windows 7 可通过网络位置这种功能有效地保护我们的安全。有关网络位置的详细信息，请参考本书 8.1.3 节网络位置。

5. 不用的时候关闭无线网络

现在很多带有无线网卡的计算机上都提供了一个用于开启或者关闭无线网卡功能的硬件开关，通过这个开关，我们可以直接启用或者禁用无线网卡。

如果笔记本上带有这样的开关，那么在不使用无线网络的时候，最好能通过开关将无线网卡彻底关闭，而不是仅仅在 Windows 中断开无线网络。这样不仅能延长电池的使用时间，而且可以进一步提高安全性。

CHAPTER

7

第 7 章　局域网安全

通常，我们常见的局域网按照物理层介质的不同，主要可以分为有线网络和无线网络两部分，无线网络的安全问题在第 6 章已经介绍过，而有线网络本身没有太多的安全问题需要注意。因此，本章主要讨论有线网络和无线网络建成后使用中的安全问题。注意，本章内容可以同时适用于这两种类型的网络。

一般情况下，人们使用局域网的主要目的就是交流数据，例如，共享文件、共享打印机、使用网络程序，或者共享互联网连接。本章的重点会放在通过局域网共享文件和打印机的安全，例如，如何设置才能让计算机在使用共享功能的同时更加安全，以及如何通过共享机制控制别人通过网络对共享数据的访问。因为在 Windows 看来，无论是文件、文件夹还是打印机，在进行共享的时候都可以当做同等的“对象”对待。因此，本章会以文件夹的共享为例进行介绍，但这些内容不仅可以用于文件和文件夹的共享，也可以用于打印机的共享。

7.1　设置共享

以前，当我们要设置共享的时候，必须在对象的“属性”对话框中打开“共享”选项卡，然后启用共享，并设置复杂的安全选项，这样不仅麻烦，而且很容易出错。为了避免这些问题，在 Windows XP 中，微软曾提出了一种叫做“简单文件共享”的共享机制，通过这种机制，共享文件的操作会更加简单，但是相应的可选的选项也变得很少，同时共享权限的设置也不够细致。

从 Windows Vista 开始，情况又有了一些变化。在 Windows Vista 中，有两种不同的共享模式，这两种模式是可以共存的，可以按照需要随时选择不同的模式使用。

到了 Windows 7 时代，在 Windows Vista 共享向导的基础之上，还增加了使用联机 ID 进行共享的新方式。

最后，为了更进一步方便文件的共享，在 Windows 7 中，我们还可以使用公用文件夹。在使用公用文件夹后，只需要将需要共享的文件复制到这样的文件夹中，任何用户，无论是本地用户还是网络用户（公用文件夹的网络共享需要预先设置），都将可以看到我们的共

享文件，同时所有的用户在查看这些文件的时候都将具有一样的权限。

7.1.1 简单文件共享和家庭组

首先了解一下简单文件共享。就像上文说到的，这种方法操作简单，但是可供控制的选项少，无法针对不同的用户设置不同的权限。

在 Windows 7 中，默认的简单文件共享（在 Windows 7 中，这种模式叫做共享向导）在保持了 Windows XP 中的简单操作外，可选的设置更多。因为在 Windows 7 中，不仅可以添加不同的账户，还可以为不同账户设置不同的共享权限。另外，在 Windows 7 中，有关文件共享有一个很大的改进，可以以文件为单位创建共享。在老版本 Windows 中，共享只能以文件夹为单位创建，也就是说，要么共享一个文件夹中的所有文件，要么该文件夹不被共享，其中的所有文件也不被共享。然而在 Windows 7 中的情况要好很多，在一个文件夹中，我们可以选择性地共享其中的某些文件，同时不共享其他文件。

在这样做之前，首先要进行一些设置，以便在本机启用共享。完整的操作步骤如下：

STEP 01 在“控制面板”中依次单击“网络和 Internet”→“网络和共享中心”，打开网络和共享中心页面。

STEP 02 在“网络”选项下，查看“网络”字样右侧标记的网络位置是什么，如果是“专用网络”，则可以启用共享（如图 7-1 所示），如果是“公用网络”，将无法使用共享。有关网络位置的详细信息，请参考 8.1.3 节的内容。

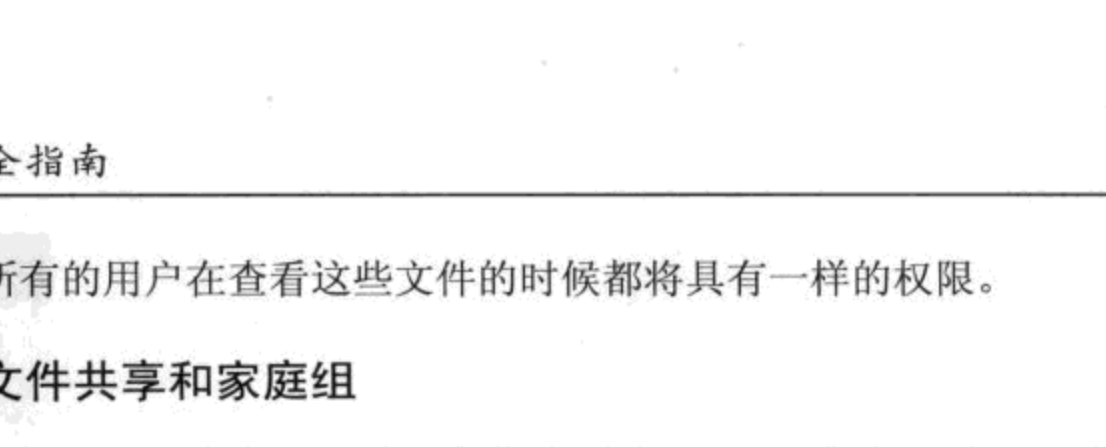


图 7-1 查看当前网络的“位置”

STEP 03 在网络和共享中心窗口的左侧，单击“更改高级共享设置”链接，随后可以看到如图 7-2 所示的设置界面。在这里，可以根据当前连接网络的类型（本例是“家庭网络”）设置更详细的工作参数。

注意，这里所做的更改将对所有该类型的网络生效。例如，如果在“家庭或工作”网络中禁用了“网络发现”功能，那么所有的此类网络，无论是以前连接过的，还是以后连接过的，只要是“家庭网络”或“工作网络”，都将禁用网络发现功能。而在针对“公用网络”启用某些功能时则需要小心，因为公用网络代表公共场所的无法被我们信任的网络，如果在这样的网络上启用某些功能，可能会降低系统的安全性。

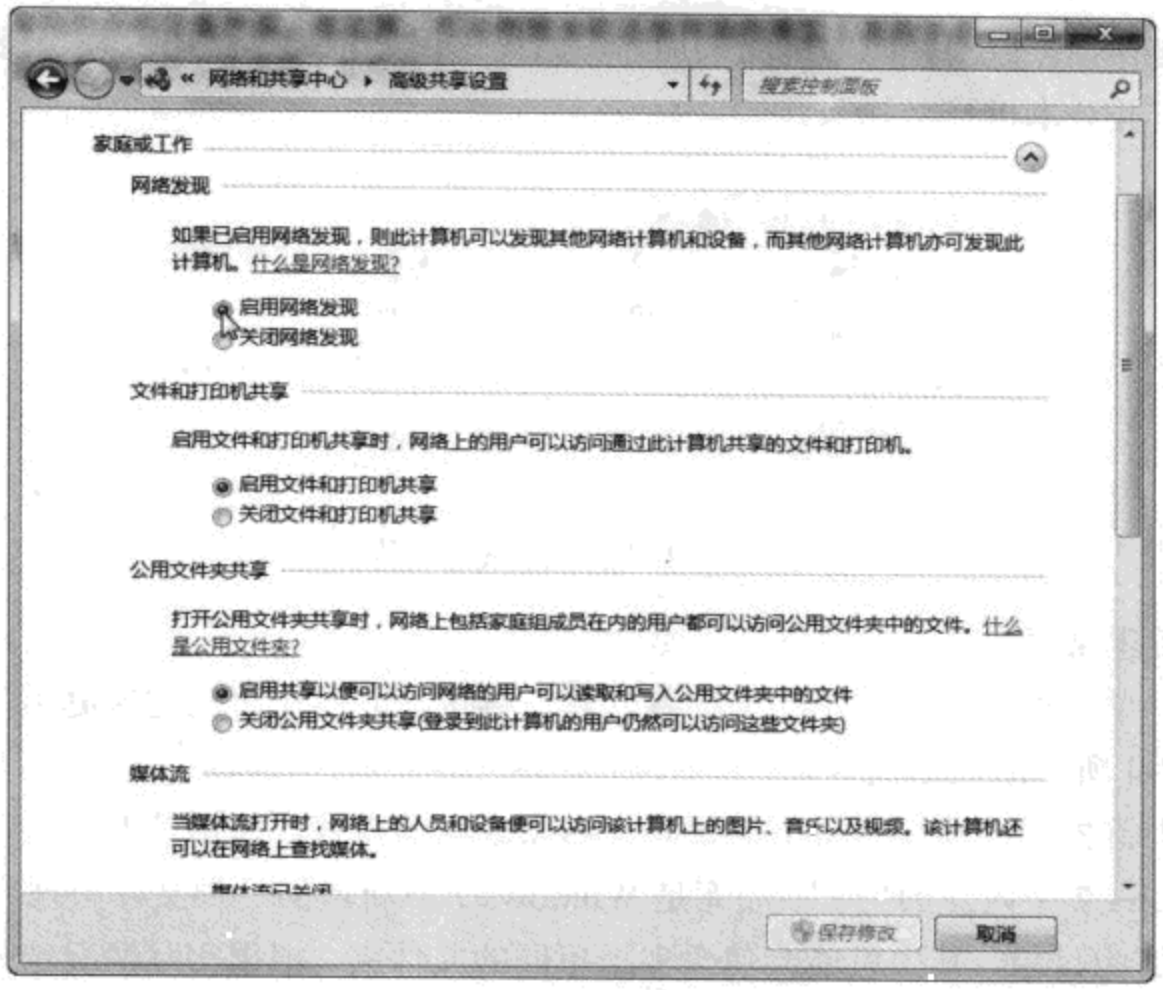


图 7-2　针对某一网络类型设置共享选项

1. 创建家庭组

在 Windows 7 中新增了一个名为“家庭组”的功能，这个功能也是为了简化局域网中的内容共享而设的。简单来说，同一个局域网中的所有计算机都可以加入同一个家庭组，随后即可将本机的资源共享给整个家庭组，并可分配不同的权限。而任何加入同一家庭组的所有计算机上的所有账户，都将可以访问这些资源。

家庭组功能的使用有下列限制：

- 同一个局域网中只能存在一个家庭组，其他计算机或者加入该家庭组，或者不加入，但不能创建多个家庭组。
- 家庭组是一种对等形式的自主网络，没有中央设备。创建家庭组的计算机在地位上与加入家庭组的计算机是一致的。假设计算机 A 创建了一个家庭组，计算机 B 加入该家庭组，随后计算机 A 从家庭组中退出，但此时这个家庭组依然是存在的。
- 如果希望将局域网中的家庭组彻底删除，必须让所有加入该家庭组的计算机全部从家庭组中退出，随后该家庭组会自动消失。
- 只有“家庭”和“工作”网络上可以创建和加入家庭组，“公用”网络上家庭组功能会被禁用。
- 加入域的计算机不能创建家庭组，但可加入现有的家庭组。

在网络和共享中心的主界面上可以看到一栏有关家庭组的内容（如图 7-3 所示）。如果这里显示为“准备创建”，则表示当前网络中不存在家庭组；如果这里显示“可加入”，则

表示当前网络存在家庭组，而本机尚未加入；如果这里显示为“已加入”，则表示当前网络存在家庭组，并且本机已经加入。

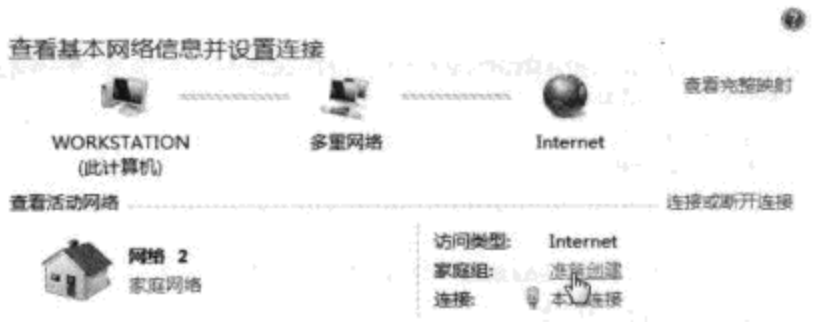


图 7-3　查看当前的家庭组使用情况

如果要新建家庭组，可按照下列步骤操作：

STEP 01 单击如图 7-3 所示的“准备创建”链接，并单击“创建家庭组”按钮，随后会打开如图 7-4 所示的创建向导。

STEP 02 首先需要选择本机上需要共享到家庭组的内容。这里需要注意，图 7-4 列出的都是 Windows 7 中内建的“库”，而库是 Windows 7 中新增的一种文件整理方式。实际上，“库”可以理解为目录，其中可能会包含多个不同的文件夹。根据实际情况选择本机需要共享的内容，然后单击“下一步”按钮。

STEP 03 稍等片刻后，向导会列出家庭组的密码（如图 7-5 所示）。其他计算机如果需要加入这个家庭组，就必须输入正确的密码。至此，该家庭组已经创建完毕，单击“完成”按钮，随后可以看到图 7-6 所示的界面，在这里可以对家庭组的其他选项进行更进一步的调整。

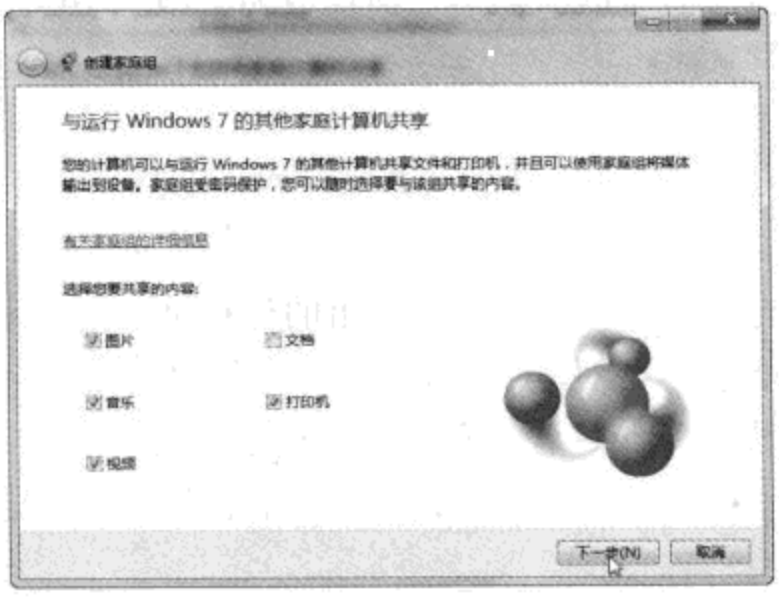


图 7-4　选择要共享到家庭组的本机内容

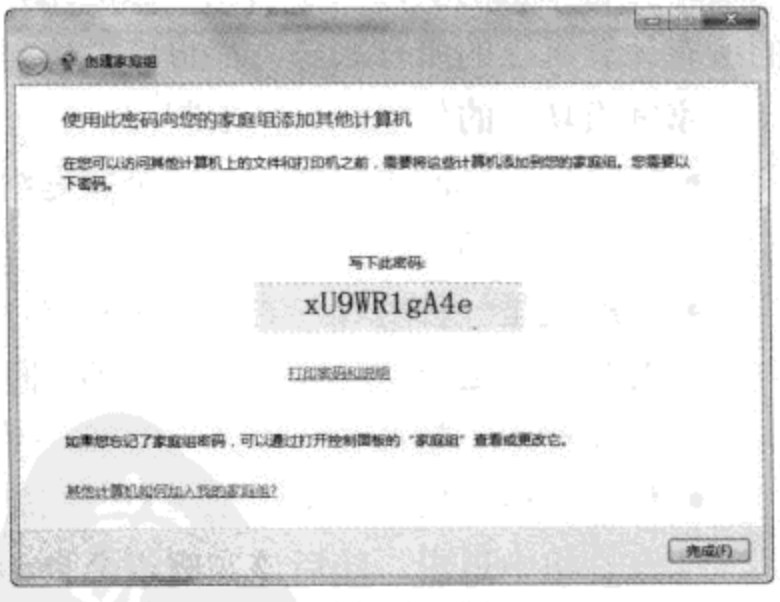


图 7-5　该家庭组的“准入”密码

STEP 04 图 7-6 中的选项与安全性最密切相关的就是家庭组的密码，因为家庭组是一种对等的自治网络，其唯一“准入”机制就是密码，任何获得该密码的人都可以将自己的计算机加入家庭组，进而获得所有共享给整个家庭组的内容（如果是无线网络，这一问题

就显得尤为关注，因此，就算要修改家庭组密码，也不要使用和无线网络相同的密码）。该密码一定要妥善保管。最理想的情况是，不要修改该密码，使用系统分配的足够复杂的密码。因为这个密码只有将计算机加入家庭组的时候才需要输入，平时使用过程中并不需要。

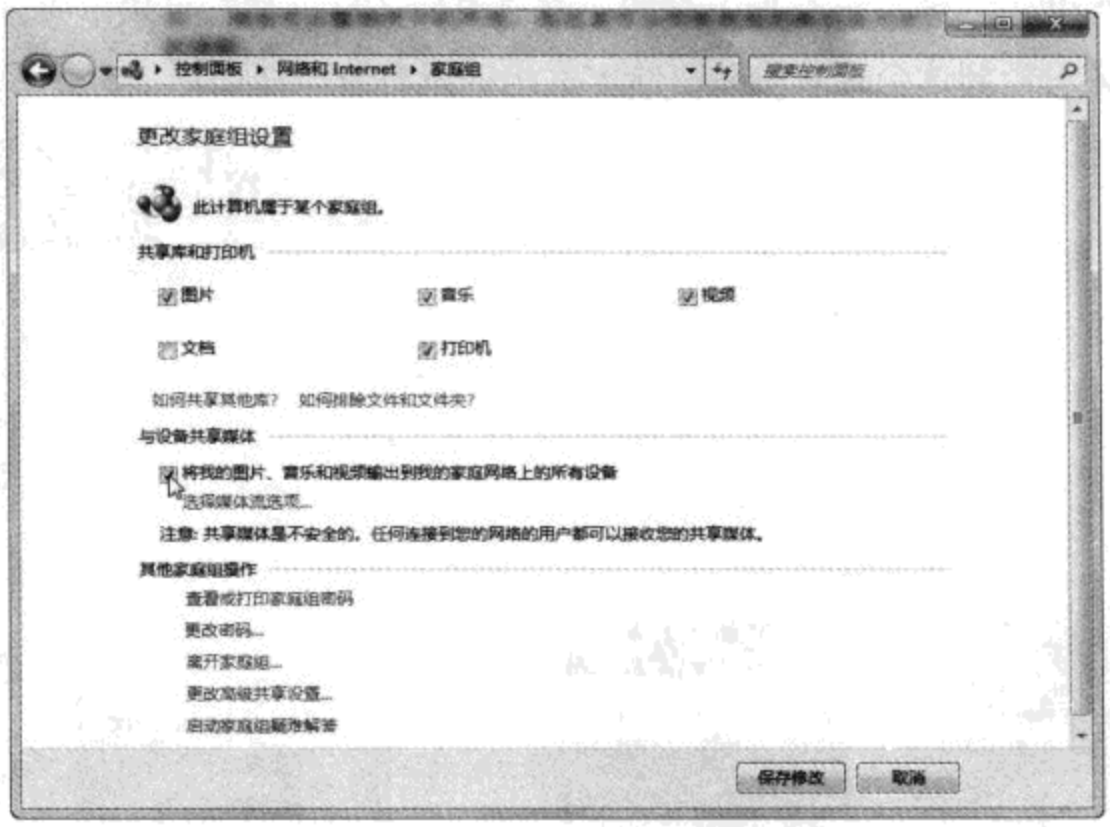


图 7-6　家庭组的其他选项

2．加入家庭组

如果需要将其他计算机加入该家庭组，可按照下列步骤操作：

STEP 01 在网络和共享中心的主页面上单击“可加入”链接，随后界面上会显示当前可加入的家庭组的创建者，以及创建时使用的计算机。如果核对无误，请直接单击“立即加入”按钮。

STEP 02 随后会看到类似图 7-4 所示的对话框，可供我们选择希望共享给整个家庭组的资源（当然也可以全部反选，不共享本机的资源）。选择好后单击“下一步”按钮。

STEP 03 接下来需要输入家庭组的密码。如果忘记了密码，可以在其他已加入该家庭组的计算机上打开图 7-6 所示的界面，并单击“查看或打印家庭组密码”链接查看。

STEP 04 输入正确的密码后，单击“下一步”按钮。如果一切无误，单击“完成”按钮退出向导。

随后，这台计算机就算是加入了家庭组，并且可以获得所有的权限，包括访问共享给家庭组的资源，以及修改家庭组密码等。

3．共享资源的创建和使用

对于加入家庭组的计算机，可以选择将资源共享给整个家庭组，或者共享给特定的用户。如果要共享给整个家庭组，只需要在 Windows 资源管理器中找到目标内容，并将其单

击选中，随后在工具栏上单击“共享”按钮，通过下拉菜单选择所需的共享权限即可（如图 7-7 所示）。

如果需要访问共享给家庭组的资源，只需打开“计算机”窗口，从左侧导航栏中单击展开“家庭组”节点，随后每台加入到同一家庭组的计算机都会显示出来，单击每台计算机的节点后，还可看到这台计算机共享给家庭组的所有资源（如图 7-8 所示）。

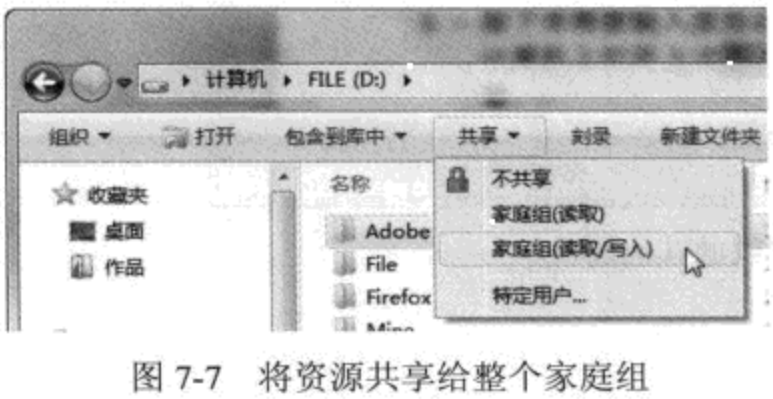


图 7-7　将资源共享给整个家庭组

图 7-8　访问共享给家庭组的资源

家庭组是一种非常方便的共享方式，但它在功能上存在一定的不足，例如，虽然可以针对共享设置访问权限为“读取”或“读取/写入”，这样的权限会对加入家庭组的任何一台计算机上的任何一个账户生效。如果希望针对某一具体账户共享资源，并设置更高级的权限，此时就不能使用家庭组功能，需要设置高级共享。

7.1.2　高级文件共享

注意，只有 Windows 7 专业版/企业版/旗舰版支持高级共享模式。不过，在同时支持这两种模式的 Windows 7 版本中，家庭组共享和高级共享这两种方式可以共存，我们可根据需要选择一种模式使用。

在 Windows 7 中，要想使用高级模式共享文件或文件夹，需要用鼠标右键单击目标对象，从右键菜单中选择“属性”，打开“属性”对话框，然后打开“共享”选项卡，单击“高级共享”按钮，随后可以打开图 7-9 所示的“高级共享”对话框。

首先需要选中“共享此文件夹”选项，随后设置共享名。共享名的选择需要注意，这里使用的名称是其他网络客户端所能看到的名称，并且可以与文件夹的实际名称不相同。另外，可以通过“将同时共享的用户数量限制为”选项设置该共享的最大并发连接数。

注意　用户数量的限制

这里所说的用户数量，是指并发访问的用户数量。简单地说，就是在同一时间访问的最大数量。对于客户端版本的 Windows 操作系统来说，在这里无论如何设置，系统都有一个默认的最大用户的数量。对于各种版本的 Windows 7，这一限制都为 20 个并发连接。这属于微软对 Windows 的硬性限制，无法突破。这样做的主要原因是，微软认为，如果并发访问用户的数量超过这个值，那么应该选择服务器版 Windows 操作系统。

随后，还需要设置共享权限，此时需要单击“权限”按钮，打开图 7-10 所示的对话框。

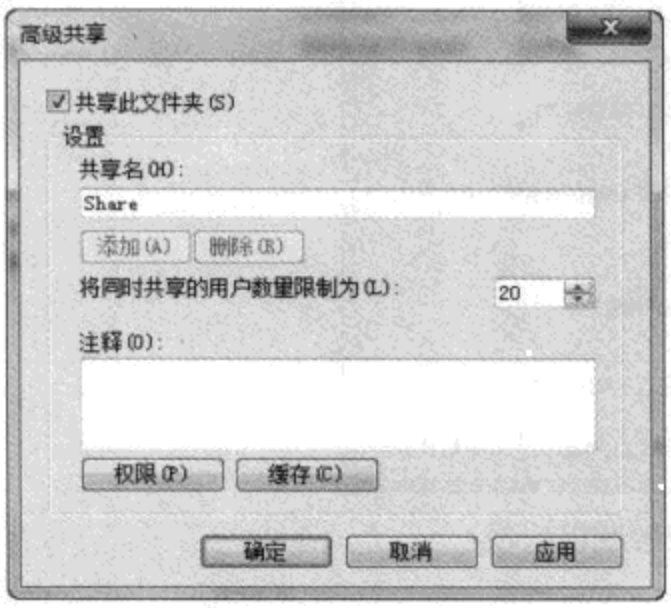


图 7-9　Windows 7 的高级共享对话框

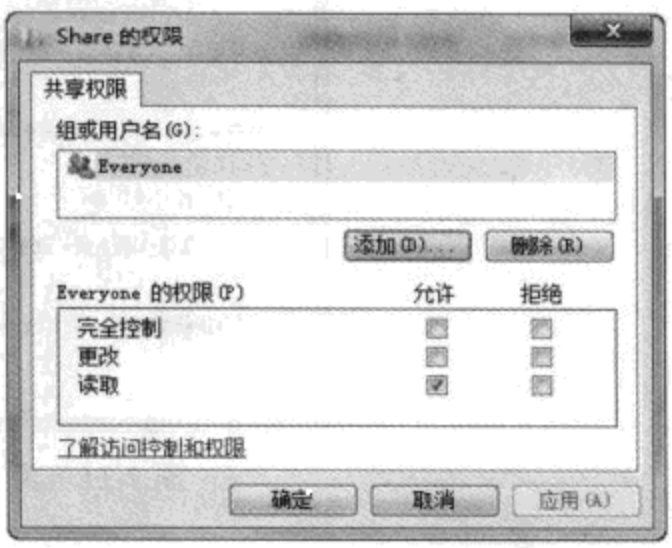


图 7-10　为共享设定高级权限

这里的内容与上文介绍的 NTFS 权限的设置方式类似。首先，通过“添加”按钮选择允许访问该共享的账户或组。随后在下方的权限列表中选择该对象可供获得的权限即可。在实际使用中需要注意，通过上述操作，系统默认会给“Everyone”分配共享权限，这将导致其他人也有可能访问该共享。因此，如果这个共享是针对某一用户的，不希望别人访问，那么一定要将 Everyone 从列表中删除。

另外，在选择用户的时候需要注意，在单机和工作组环境中，只能针对本机存在的账户设置共享权限，而别人在通过网络从其他计算机访问本机的共享时，也必须输入本机现有的账户和密码，才能通过身份验证。与共享有关的很多权限问题实际上都是因为没有认清这一点导致的，这个问题将在下文中详细讨论。

在图 7-9 所示的对话框中单击“缓存”按钮后，还将看到图 7-11 所示的内容，这些又是什么意思？

所谓脱机选项，实际是 Windows 的脱机文件夹功能。那么什么是脱机文件夹？请假设这样的情况：公司里的业务数据统一保存在一台集中的服务器上，所有的员工在工作的时候都需要连接到服务器访问这些文件，并在需要的时候做出更改，随时保存在服务器上。假如某个员工要出差，并且在出差的过程中需要访问公司的这些文件，这时候该怎么办？

如果是以前，他可能只能将文件从公司的文件服务器上复制到本地硬盘，然后带着这些数据出差，一旦在出差过程中修改了某些文件的内容，等回到公司后还要手工将修改的文件重新复制到服务器上，这种做法不仅烦琐，而且很容易出错或者造成遗漏。尤其是如果在出差的过程中，公司里其他同事编辑了某个文件，他在外面也编辑了同一个文件的不同内容，那么在将文件复制回服务器的时候，还要浪费时间判断每个文件的版本，这就更加麻烦了。

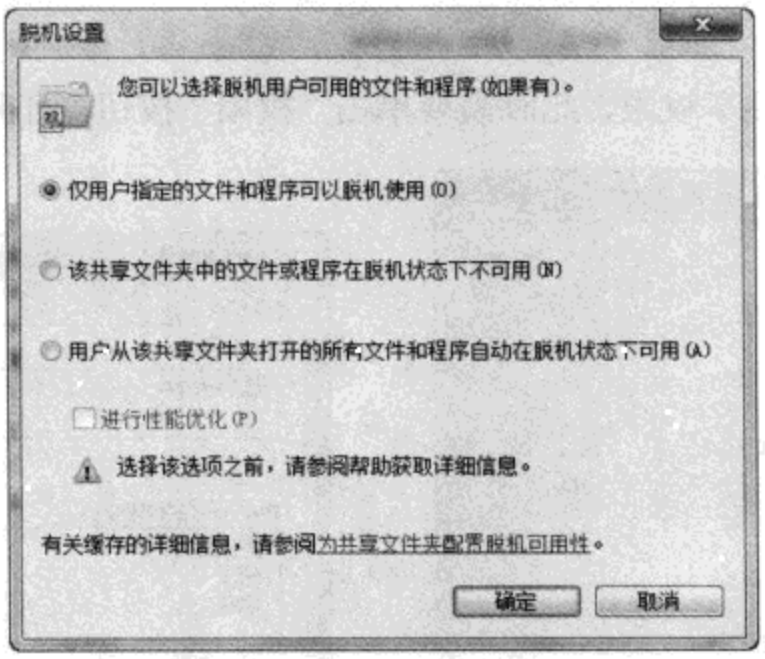


图 7-11　为共享设置脱机选项

如果使用脱机文件功能，一切都将迎刃而解。脱机文件就好像将网络服务器上的文件在本地硬盘上创建了缓存，在可以访问网络的时候，直接访问网络服务器上的最新版本，但在断开网络后，依然可以像网络正常的时候那样，使用同样的网络路径访问同样内容的文件，并可以在需要的时候对文件进行修改（前提是具有修改的权限）。当网络恢复正常后，Windows 还可以自动将本地的缓存和网络服务器上的文件进行比较，并将被编辑过的文件进行同步。

缓存设置就是用于控制脱机文件功能的。和脱机文件功能的不同之处在于，脱机文件功能中，是由通过网络访问该文件的用户决定是否使用脱机文件，以及如何同步的；而缓存设置是由创建该共享的用户决定访问这些共享的人是否脱机使用，以及如何同步的。

单击“缓存”按钮后，可以看到图 7-11 所示的“脱机设置”对话框，这里列出的选项内容和含义分别是：

- 仅用户指定的文件和程序可以脱机使用　如果选择该选项，那么允许内容被脱机使用，但必须由访问该内容的用户自己决定对什么资源脱机使用。如果希望脱机使用，只需要通过网络打开该共享资源，鼠标右键单击希望脱机使用的文件夹，然后选择“始终脱机可用”即可。
- 该共享文件夹中的文件或程序在脱机状态下不可用　如果选择该选项，则意味着禁止用户脱机使用该资源，此时鼠标右键菜单中的“始终脱机可用”选项将是灰色的。

- 用户从该共享文件夹打开的所有文件和程序自动在脱机状态下可用　如果选择该选项，则意味着内容允许脱机使用，并且不需要其他用户亲自设定，只要曾经打开过该共享中的内容，就会被自动设置为可脱机使用。

如果需要访问通过这种方式共享的资源，则需要在“计算机”窗口中单击导航栏内的“网络”节点，并进入目标资源所在的计算机，然后才能访问。

7.1.3　公用文件夹

除了直接将硬盘上保存的文件或文件夹在自己所在的位置共享出来外，还可以将需要共享的文件复制到公用文件夹中，以实现和本机的其他账户或者网络用户共享文件的目的。

公用文件夹是一个比较特殊的系统文件夹，该文件夹会被默认共享给本机的所有用户，并且所有的本机用户都可以向其中复制文件，而通过设置，所有的网络用户都可以直接访问该文件夹中的内容。不仅如此，还可以为共享文件夹设置访问权限，这样所有的网络用户都将具有一样的访问权限。

对于 Windows 7，公用文件夹的使用更简单。默认情况下，公用文件夹位于“\Users\Public”目录下，并且这些内容都包含在每个账户的“库”中。例如“公用文档”被包含在每个用户的“文档”文件夹中，“公用音乐”包含在每个用户的“音乐”文件夹中。因此，对于本机的所有用户，都可以直接通过“库”访问所有的公用文件夹（如图 7-12 所示）。

如果希望自己的内容被本机的其他用户直接读写，可以将内容复制或移动到公用文件夹中。

默认情况下，Windows 7 中的公用文件夹也只能被所有的本机账户访问。如果希望其他网络用户可以访问，则需要进行一番设置。详细的步骤如下：

STEP 01　在“控制面板”中依次单击“网络和 Internet”→“网络和共享中心”，打开“网络和共享中心”页面。

图 7-12　每个人的“库”中都包含了来自公用文件夹的内容

STEP 02 在窗口左侧单击“更改高级共享设置”链接，展开“家庭或工作”节点，然后选中“启用共享以便可以访问网络的用户可以读取和写入公用文件夹中的文件”选项。

在介绍了公用文件夹和用户自己创建的共享文件夹后，有人可能会考虑，到底什么情况下使用公用文件夹，什么情况下使用自己创建的共享文件夹来共享文件。其实这个问题可以根据文件的用途来决定。

假设家庭环境中有一台计算机上保存了很多数码照片，其他家庭成员希望能够在自己的计算机上通过共享的方式直接查看这些照片，那么与其将保存了照片文件的文件夹共享出来，还不如直接将所有的照片直接保存到公用文件夹中，这样至少本机的所有账户都将可以直接访问，而一旦设置了共享公用文件，局域网中其他计算机上的用户也将可以直接访问。

对于比较机密的或者私人的文件，如果不希望每个人都能看到，但希望共享给特定的某个人，这种情况下，直接共享这些文件所在的文件夹，并设置合理的共享权限则是更合理的方法。

7.1.4 管理共享

在共享了大量保存在不同位置的文件夹后，希望知道自己有哪些文件夹都被共享了出去呢？硬盘突然繁忙了起来，怀疑是有人正通过网络复制比较大的文件，但又不知道自己的判断是否准确？想要知道目前都有哪些人在访问共享文件，分别访问了哪些文件？这些工作其实并不需要借助什么特殊的工具或者高深的知识，利用 Windows 自带的工具完全可以做到。

这里需要使用的是计算机管理控制台中的共享文件夹管理单元。在“计算机”上单击鼠标右键，选择“管理”，即可打开“计算机管理控制台”窗口，在窗口左侧的控制台树中展开“计算机管理”→“系统工具”→“共享文件夹”(或者也可以直接运行 compmgmt.msc)，本节就要用到这里提供的功能。

7.1.4.1 查看和管理共享

如果希望查看本机上都有哪些共享，并且希望查看这些共享的具体设置，或者希望在一个集中的界面下统一调整所有共享的设置，这时候可以进入共享文件夹控制台的“共享”节点，这里列出了本机上的所有共享，不仅包括用户自己创建的，还包括系统默认的共享(如图 7-13 所示)。

例如，从“文件夹路径”一栏可以知道该共享到底是将本地硬盘上的哪个文件夹共享了出来，而从“客户端连接”一栏可以知道当前有几个网络用户在访问该共享。

如果用鼠标右键单击一个共享，那么在右键菜单中还有更多的选项可以使用。例如，单击“打开”选项可以使用 Windows“资源管理器”打开该共享对应的文件夹位置；单击“停止共享”选项可以取消对目标文件夹的共享；单击“属性”选项后可以调整该共享的设

置，因为所有设置的内容和创建共享时的选项完全一样。因此，大家可以参考上文了解如何调整这些设置。

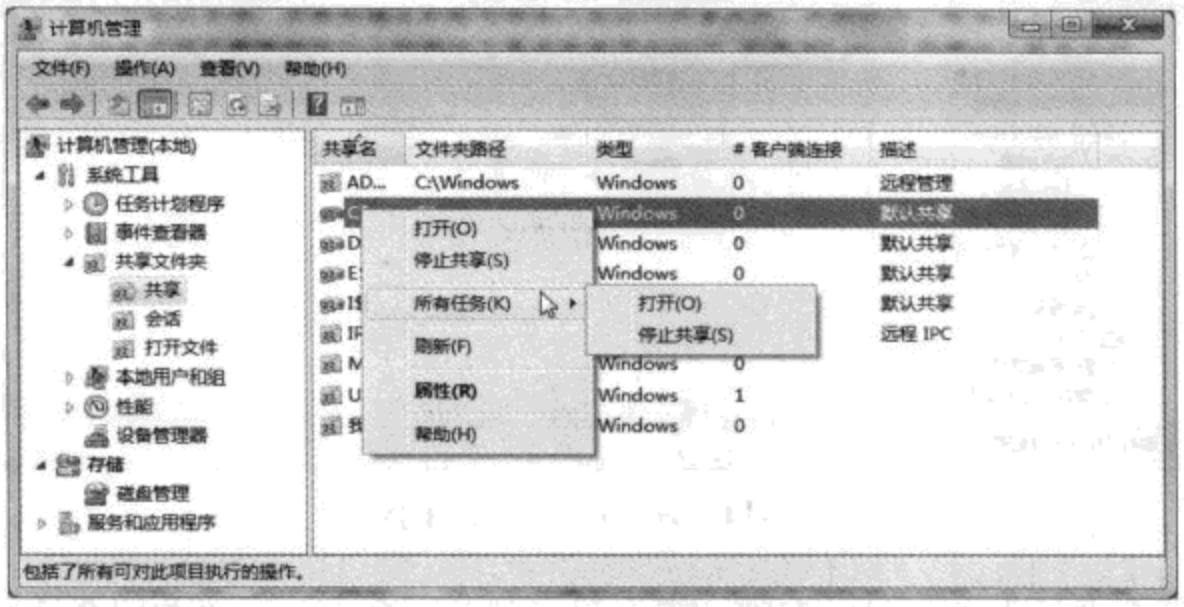


图 7-13　查看本机已创建的所有共享

在“共享”节点下，如果用鼠标右键单击右侧窗格的空白处，那么弹出菜单中还会出现“新建共享”命令，使用该命令可以打开创建共享文件夹向导，这个向导可以指导我们一步步地完成创建共享需要设置的所有步骤，同样，这些操作和上文介绍的创建共享的操作几乎完全一样，只不过这里使用向导的形式将所有的操作整合到了一个界面上，更加便于使用。

另外，创建共享文件夹向导还使得我们可以直接将远程计算机上的文件夹共享出来。还可在“计算机管理控制台”窗口中，在左侧控制台树上的“计算机管理（本地）”节点上单击鼠标右键，选择“连接到另一台计算机”，在随后出现的“选择计算机”对话框中选择本地局域网中的其他计算机，并输入该计算机上管理员账户的密码，这时原本的“计算机管理（本地）”节点就会变成“计算机管理（远程计算机的名称）”，再次进入“共享”节点，就可以直接远程管理其他计算机上的本地共享，并可以在需要的时候新建共享。

7.1.4.2　查看和管理会话

如果远程用户连接到本机，那么他就和本机创建了一个会话。要想知道当前都有哪些用户和本机建立了会话，可以进入到共享文件夹控制台组件的“会话”节点中，随后，右侧窗格就会显示所有和本机建立了会话的用户，以及这些用户的详细信息（如图 7-14 所示）。

这里可以重点关注几个内容，“用户”一栏显示了远程用户使用本机的哪个账户身份通过了验证（关于这一点，请参考 7.2.1 节网络用户的身份验证），“计算机”一栏显示了远程计算机的名称，而“打开文件”一栏显示了该会话打开的文件数量，“连接时间”一栏显示了该会话创建并持续的时间，“空闲时间”显示了该会话有多长时间没有活动了，“来宾”一栏显示了该会话是否被验证为 Guest 账户。

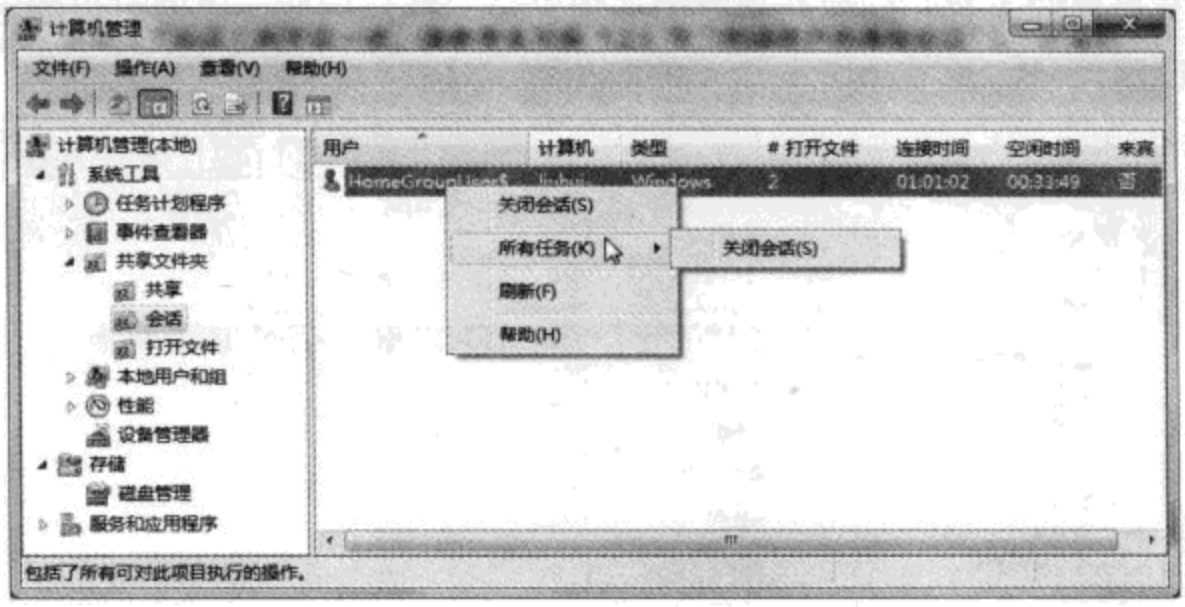


图 7-14　查看和管理 SMB 会话

如果在某个会话上单击鼠标右键，那么弹出菜单中会有一个“关闭会话”选项，单击该选项后，这个会话就会被自动关闭。同时，如果想要一次关闭所有的会话，则可以用鼠标右键单击右侧窗格的空白处，然后从弹出菜单中选择“中断全部的会话连接”。实际进行该操作的时候需要注意，如果对方打开了我们的共享文件，并进行了编辑（如果具有相应的权限），在没有保存的情况下又中断了会话，就有可能导致对方的数据丢失。

7.1.4.3　查看和管理打开的文件

除了可以看到有哪些计算机与本机建立了会话外，在“打开文件”节点下还可以看到每个网络用户具体在查看本机的哪个文件或文件夹。进入“打开文件”节点后，可以看到图 7-15 所示的界面。

例如，在“打开文件”一栏可以看到对方打开的文件或文件夹的路径，在“访问者”一栏，可以看到远程用户使用本机的哪个账户的身份通过了验证，在“打开模式”一栏可以看到对方进行的是哪种操作。

如果在某个会话上单击鼠标右键，那么弹出的菜单中会有一个“将打开的文件关闭”选项，单击该选项后，这个打开的文件就会被自动关闭。同时，如果想要一次关闭所有打开的文件，那么可以用鼠标右键单击右侧窗格的空白处，然后从弹出菜单中选择“中断全部打开的文件”。实际进行该操作的时候需要注意，如果对方打开了我们的共享文件，并进行了编辑（如果具有相应的权限），在没有保存的情况下又中断了会话，就有可能导致对方的数据丢失。

这里需要注意一点，关闭一个打开的文件后，该文件在对方的计算机上还是存在的。这个功能并不是说在关闭打开的文件时，对方计算机上的该文件也会消失，这里我们关闭的只是对方计算机到本机的这个连接而已。

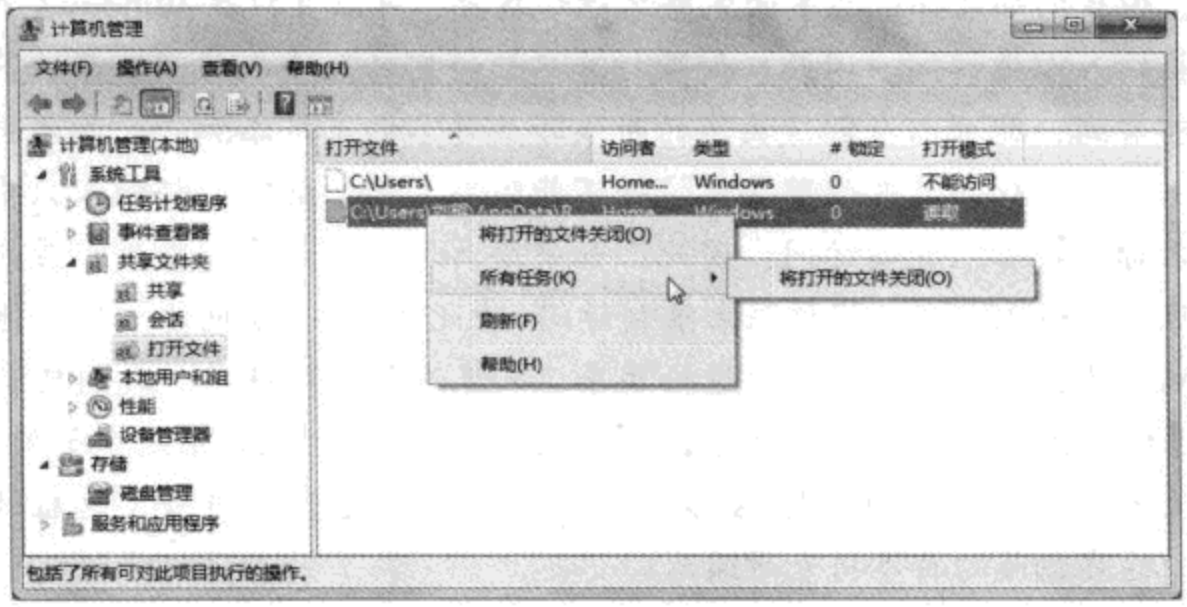


图 7-15　查看和管理打开的文件

7.1.5　默认的管理共享

在使用共享文件夹管理单元的共享节点查看本机上的共享时，有人可能已经发现了一些奇怪的共享，这些共享的共享名末尾都有一个美元符号（$），它们并不是我们自己创建的。其实，它们是 Windows 操作系统默认的管理共享，这些共享是做什么用的，我们是否应该将其全部删除？

所谓的管理共享，顾名思义，就是用于管理的共享。例如，企业网络的管理员可以连接到远程计算机，直接修改远程计算机的注册表，或者使用计算机管理控制台连接到远程计算机，配置远程计算机的各种选项。这些工作就需要用到系统默认的管理共享。除此之外，如果在网络中使用了某些管理软件，那么为了使这些软件可以正常工作，也需要用到管理共享。通常来说，Windows 操作系统中默认的管理共享有以下这些：

- **硬盘分区或卷**　例如 C$、D$等，默认情况下，每个本地硬盘分区都有一个这样的管理共享，这个共享主要是为了让管理员直接通过网络访问到远程计算机上的文件。
- **系统文件夹**　例如 ADMIN$，其实这个共享对应的文件夹是 Windows 主目录，这个共享的主要作用是为了让管理员可以用更便捷的方法访问 Windows 系统文件。
- **FAX$**　这个共享主要用于缓存传真客户端发送的传真。
- **IPC$**　这个共享主要用于通过使用命名管道在网络程序之间通信的客户端与服务器之间的临时连接。
- **PRINT$**　这个共享主要用于远程管理打印机。

> **注意**　用美元符号隐藏共享
>
> 有人可能已经在纳闷了，既然这些管理共享是默认就有的，那么我们在网上邻居中打开远程计算机后，为什么看不到这些共享？其实这就是共享名末尾的美元符号（$）的功劳。按照设计，Windows 操作系统并不显示共享名末尾带有美元符号的

> 共享，但我们如果知道共享的完整名称和路径，可以直接在 Windows 资源管理器的地址栏输入以便访问。因此，如果打算只让特定的几个人访问共享，甚至不希望别人能够看到，就可以在创建共享的时候给共享名的末尾添加一个美元符号。但需要注意一点，这样做只能隐藏共享，并不能限制人们的访问。任何人只要知道隐藏共享的名称，就可以直接访问，因此，如果要共享比较机密的数据，最好能够通过共享权限并配合 NTFS 访问权限来限制访问。除此之外，如果网络中有其他非 Windows 客户端计算机也需要注意，通过给共享名末尾添加美元符号，我们只能让 Windows 操作系统无法直接显示这些共享，但其他非 Windows 操作系统中如果安装了 SMB 组件（主要用于访问 Windows 操作系统上的共享文件），在查看远程计算机上的共享时，这些隐藏的共享将无所遁形。

既然默认的管理共享的主要作用是用于系统的管理，那么是否可以通过禁用这些共享来提高 Windows 的安全性？这需要分情况讨论，首先需要明白的一点是，这些既然是管理共享，那么就决定了只有管理员可以访问这些共享。因此，只要计算机上的管理员账户都受到强密码保护，别人就算知道启用了管理共享，因为没有管理员账户的密码，也无法访问。尤其是在企业网络环境中，有时候这些管理共享是实现某些操作所必需的，因此，不能也不建议将其删除。

如果不需要使用网络管理功能，或者只有一台计算机，本着**“最少的服务等于最大的安全”**这一原则，还是可以将这些共享全部删除。运行 regedit 打开注册表编辑器，定位到 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters，在这里找到两个名为“AutoShareServer”和“AutoShareWks”的 DWORD 值（如果不存在，则可以自己创建），然后将这两个值的数值都修改为“0”，重启动后，该设置就可以生效。日后如果需要使用管理共享，也只需要将这两个值的数值修改为“1”即可。

> **注意** 在使用这种方法禁用了管理共享后，如果计算机在执行原本正常的操作时突然遇到了某些莫名其妙的问题，请优先考虑是否是禁用了管理共享导致的，可以暂时重新启用，以便排查问题。

7.2 控制数据的访问

上文已经介绍了如何创建共享，那么到底该怎样控制网络用户对共享数据的访问？这是本节要介绍的内容。需要注意的是，本节内容要求使用高级文件共享模式。同时，为了能够让共享权限和 NTFS 访问权限配合使用，还要求所用的 Windows 版本必须能支持设置 NTFS 权限。

7.2.1　网络用户的身份验证

要想成功地访问到一台计算机上的共享文件，我们必须能够提供有效的用户凭据（用户名和密码），并且要能够通过 Windows 的验证，因为只有这样，Windows 才知道应该给这个网络用户怎样的访问权限。在这个过程中涉及了很多后台的操作，同时在访问共享文件方面，我们遇到最多的问题都是在这个过程中出现的。

例如，在访问共享文件的时候，Windows 甚至根本不要求我们输入用户名和密码，就告诉我们缺少所需的权限，这些问题是怎么发生的，又该怎样解决？

让我们先来看看访问共享的时候身份验证的整个过程。假设用户 A 需要从计算机 A 上访问保存在计算机 B 上的一个共享，那么在进行身份验证的时候，计算机 B 首先会根据用户 A 提供的凭据判断是否允许用户 A 通过网络访问计算机 B。如果允许访问，那么用户 A 随后可以看到计算机 B 上的所有共享。当用户 A 双击试图打开某个共享 C 的时候，计算机 B 首先会根据用户 A 提交的凭据信息和共享 C 的共享权限设置，判断是否允许用户 A 访问共享 C，如果允许，还会判断给用户 A 怎样的共享权限。接下来，在用户 A 打算访问的时候，计算机 B 还会根据共享 C 中的文件的 NTFS 权限设置再次检查是否允许用户 A 访问，以及用户 A 可以获得怎样的权限。

从上面的过程可以看出，在判断用户是否可以访问，以及决定有效权限的时候，需要同时考虑共享权限和 NTFS 权限的设置。同时，用户 A 可以提供怎样的访问凭据对最终的结果起到了决定性的作用。

下面来看看用户在访问网络共享的时候可以提供怎样的访问凭据。在本书的第一部分介绍用户账户的时候曾经提到过，在 Windows 中主要有两种类型的用户账户：本地账户和域账户，那么账户类型的不同对访问共享时身份验证的操作有什么影响？我们都知道，对于本地账户，账户的用户名和密码等凭据信息是保存在本地安全数据库（SAM）中的，用户在登录 Windows 的时候，系统都会将用户输入的用户名和密码等信息和本地 SAM 中保存的信息进行比较，如果找到一致的条目，才允许登录，否则会被拒绝。

那么网络用户远程访问本机文件的时候，用户的身份是如何确定的？假设计算机 A 上的用户 A 试图访问计算机 B 上的一个共享，计算机 B 首先会验证用户 A 的身份。和很多人想象中的不同，在这种情况下，取决于计算机 B 的设置，用户 A 有两种选择：被验证为计算机 B 上的 Guest 账户，或者被验证为计算机 B 上的一个本地账户。也就是说，用户 A 在通过计算机 A 访问计算机 B 上的共享时，如果不希望被验证为 Guest，那么用户 A 必须有一个计算机 B 上的有效账户的用户名和密码，并在需要的时候输入到“登录”对话框中。

窍门　如何设定验证为 Guest 或者其他账户

如果希望所有访问本机共享的用户直接被验证为 Guest，需要在高级共享设置中关闭“密码保护的共享”；如果希望所有访问本机共享的用户被验证为其他账户，并为不同账户设定不同的访问权限，则需要启用“密码保护的共享”。

对于单机或工作组环境下的 Windows 局域网，这是一个比较麻烦的问题。但对于域环境情况下，则会稍微简单一些，因为在域环境下，大家都使用域账户，而域账户的登录信息保存在域控制器上。因此，用户 A 完全可以使用自己的域账户登录到计算机 B（只要这台计算机也加入了域），计算机 B 会将用户 A 提交的域账户信息提交到域控制器上进行验证。

本书重点讨论的是单机和工作组环境下的本地账户的验证问题。对于数量很少的计算机组成的工作组网络，这里有一个比较简单的方法，在需要共享文件的计算机上创建一个专门用于访问共享文件的账户，并为该账户设定一个密码，然后将该账户的用户名和密码告诉所有需要访问本机上共享文件的用户。这样，每个需要访问共享的用户在自己的计算机上打开本机的共享时，只要输入这个专用账户的用户名和密码，即可获得相应的访问权限。这种方法比较麻烦，但确实是一种比较有效的方法。尤其是如果我们需要为不同用户设定不同的访问权限时，就需要在本机创建多个本地账户。

窍门　禁止这些账户本地登录

假设我们在本机上创建了几个专门用于访问共享的本地账户，并且希望这些账户只用于访问本机上的共享，而不希望别人使用这些账户进行本地登录，则可以配置本地安全策略。详细信息请参考本书第 3 章策略安全中有关“拒绝本地登录”策略的内容。

另外，如果不需要为不同的网络用户设定不同的共享访问权限，那么将所有的网络用户都验证为 Guest，并为 Guest 账户设定所需的共享权限也是一种解决办法。

7.2.2　管理保存的密码

在访问远程计算机上的共享时，如果对方的计算机被配置为需要验证用户身份，那么，我们将会看到类似图 7-16 所示的“输入网络密码”对话框，在这个对话框中输入对方计算机上一个本地账户的用户名和密码，即可登录到对方的计算机，并查看对方所有的共享。

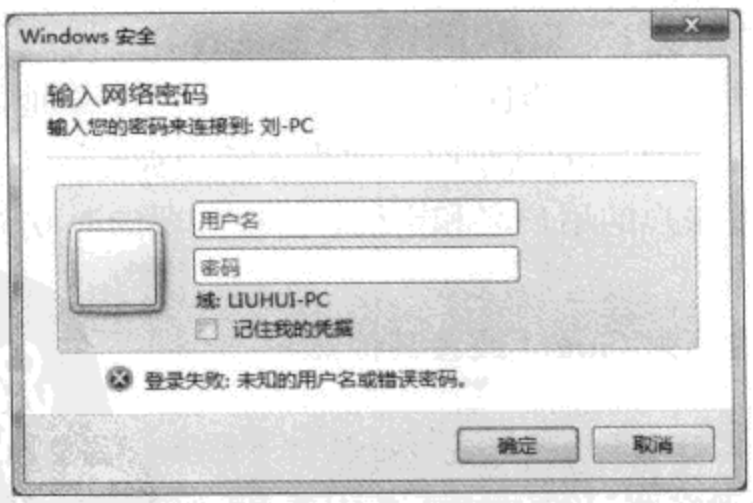


图 7-16　访问网络共享时的登录对话框

如果希望以后访问同一台计算机上的共享时不再需要输入密码，可以选中“记住我的凭据”选项。但如果在选择记住密码后因为某些原因又希望不再记忆密码，这时候该怎么办？难道在对方的计算机上更改这个账户的密码，让记住的老密码失效，以后使用新的密码登录？其实有更简单的办法，此时可参考本书 2.4 节的内容，因为访问网络共享记住的密码都属于 Windows 凭据，可直接进行修改或删除。

7.2.3　共享权限和 NTFS 权限的配合

解决了远程用户的身份验证问题后，用户远程访问本机上的共享时，最终获得的访问权限是怎样的？这里需要同时考虑共享权限的设置和 NTFS 权限，因为最终的权限将同时受到这两种权限的影响，同时网络用户可以得到的最终权限将会是共享权限和 NTFS 权限结合后的最小权限，同时拒绝权的优先级最高。

在继续之前，让我们首先看看有哪些共享权限可以设置。在 Windows 7 中使用高级共享模式时，可用的共享权限按照权限的大小排列，共有“完全控制”、“更改”和“读取”三种。那么 NTFS 权限有多少种类，详细信息请参考本书第 5 章中表 5-1 的介绍。

下面用一个例子来说明。假设有一个名为“File”的文件夹，位于 NTFS 分区上，针对 Users 组用户，其 NTFS 权限设置如图 7-17 所示。从图中可以看到，Users 组的用户对该文件夹具有读取和执行、列出文件夹目录，以及读取权限。

将该文件夹共享后，在设置共享权限的时候，添加本机的 Users 组，只选择“读取”权限，随后让别人通过网络访问该共享，并且使用一个本机的 Users 组账户进行身份验证。该用户完全可以看到所有的文件夹和文件内容，但当他试图修改文件内容、删除文件，或者新建文件和文件夹的时候，就会被报告缺少权限。很明显，在这个例子中，共享权限的设置明显小于 NTFS 权限，因此，用户将只能获得较小的共享权限设置。

图 7-17　File 文件夹的 NTFS 权限设置

这里需要注意一点，在上面的例子中，这个 Users 组的用户只有在通过网络访问该共享的时候会因为共享权限的设置而受到限制。如果有人使用该账户在本机上进行了本地登录（坐在本机前使用本机的键盘和鼠标登录），这时候，他对 File 文件夹的访问将只受到 NTFS 权限的限制，共享权限此时将不再生效。为了避免这个问题发生，应该通过安全策略拒绝专用于共享的账户的本地登录权限。

同理，如果某个文件夹的共享权限给一个用户指派了完全控制的权限，但 NTFS 权限只给这个用户指派了读取的权限，最终取小后，该用户将只能获得“读取”的 NTFS 权限。

CHAPTER

8

第 8 章　网络防火墙

现在连接到互联网的计算机越来越多，而互联网上的风险也很多。因此，很多情况下，反病毒软件、网络防火墙，以及反间谍软件成了保护我们信息安全的三个主力军。本章主要关注 Windows 中自带的网络防火墙软件。

很久以来，Windows 都不自带网络防火墙，通常都需要自行安装。然而从 Windows XP 开始，微软第一次给 Windows 系统中捆绑了一个叫做 Internet 连接防火墙的网络防火墙，从 Windows XP SP2 开始，该防火墙被改名为 Windows 防火墙。在 Windows XP 之后，Windows Vista/7 都包含这一防火墙。

在 Windows 7 中，除了传统的 Windows 防火墙外，微软还增加了一个以组策略形式配置的高级安全 Windows 防火墙，该防火墙可供配置的功能更多，但在使用上也更加复杂。好在绝大部分情况下，使用 Windows 防火墙可获得妥善的网络保护。

在继续下文之前，首先要提到很多人一个很不好的习惯，这种习惯更常见于安装了专用硬件防火墙的企业网络环境中。因为在这种环境下，很多人都认为，既然已经在网络外围统一安装了硬件防火墙，那么局域网内部的计算机上就不用再安装了，否则不仅影响速度，还可能会让某些企业应用程序的配置变得更加复杂。这种想法在现在的实际环境中已经严重落伍了。

假设这样的情况：某家企业的 IT 人员非常尽职，在企业网络的边缘部署了很好的硬件防火墙，保护了整个企业网络的安全，因此，网络中的所有客户机都没有安装额外的防火墙软件。一天，有位员工到客户的公司开会，并带去了自己的笔记本电脑。然而客户公司的网络维护有些问题，网络中有的计算机中了蠕虫病毒，并不时地向整个网络中传播，这位员工带去的笔记本电脑因为反病毒软件忘记了升级病毒定义，无法检测到这种病毒，进而导致在连接到客户公司的网络后立刻被蠕虫病毒感染。等员工回到自己公司，并将自己的笔记本接入网络后，整个公司网络立刻被蠕虫病毒感染，企业的关键业务甚至也一度中断。

因此，无论觉得自己的网络有多么安全，在所有的客户端计算机上安装网络防火墙都是很有必要的（该道理也适合于反病毒软件）。如果是出于节约投资或者担心网络防火墙影响速度的原因考虑，至少也建议启用 Windows 自带的防火墙，Windows 防火墙本身就是

Windows 的一部分，在购买 Windows 授权的时候已经包含了使用该防火墙的费用，同时该防火墙对系统资源的占用也是相当低的。

8.1　Windows 防火墙

在安装好 Windows 之后，Windows 防火墙就已经在保护我们的系统了，因为该功能默认就是被启用的。同时，很多人在使用 Windows 的过程中可能已经发现，Windows 防火墙和第三方的防火墙软件相比有一个很大的不同，Windows 防火墙很少对用户有“喋喋不休”地询问。例如，在某个程序打算访问网络的时候，其他防火墙可能会询问我们是否允许该程序访问，而 Widows 防火墙在绝大部分情况下并不会征求我们的意见，只有在一些特殊的情况下才会发出询问。

这是因为它和第三方防火墙的工作原理不同，大部分其他防火墙的工作原理是数据包过滤，这类防火墙是根据接收到的数据包的内容来判断是否允许数据包通过防火墙，而 Windows 防火墙属于静态过滤防火墙，简单来说，只有在 Windows 防火墙确认这个数据包是由本机的某个程序响应并收到的才会允许通过，如果收到的某个数据包是没有经过本机运行的程序发起，而是直接接收到的（在 Windows 防火墙中，这类连接叫做“未经主动请示的传入连接”），这时 Windows 防火墙才会对用户进行询问。

这种工作原理让 Windows 防火墙显得更好用，因为用户不再需要应对喋喋不休的询问，防火墙已经在后台帮助我们自动处理了大部分的过滤工作，只有在确实有必要的时候才会发出询问。然而这种静态过滤防火墙也存在一个很大的不足：无法直接对程序的网络访问进行控制，例如无法禁止某个程序主动访问网络。因此，请根据自己的实际需要决定是否使用 Windows 防火墙。不过对于有一定技术水平的用户，还可以使用高级安全 Windows 防火墙对程序的主动网络访问进行限制，详细信息请参考下文。

8.1.1　启用和禁用防火墙

Windows 防火墙默认是被启用的，同时也建议使用它，但有时可能依然需要禁用 Windows 防火墙。例如，打算安装第三方防火墙软件，为了避免冲突，最好首先将 Windows 防火墙禁用，或者因为某些原因必须禁用所有的网络防火墙。

在 Windows 7 中，请打开“控制面板”，依次单击“网络和 Internet”→“网络和共享中心”→“Windows 防火墙”，随后将打开图 8-1 所示的 Windows 防火墙界面。

在 Windows 7 中，Windows 防火墙最大的改进在于可同时支持多个配置文件。默认情况下，Windows 7 自带有三个配置文件，分别适用于专用网络、公用网络，以及域网络（只有加入域的计算机上才会出现与域网络有关的内容）。虽然 Windows Vista 也是这样做的，但它在同一时间只能使用一个配置文件，具体使用哪个则取决于所连接的网络的具体类型。

图 8-1　Windows 防火墙的主界面

大部分情况下，这种设计没什么不妥，但现在的计算机可能的连接方式越来越多，已经不再像以往那样单一。例如笔记本电脑，可以通过有线网络连接到公司的域环境，但同时可能还在使用内置的 3G 模块连接到运营商的 3G 无线网络。在这种情况下，使用同一个防火墙配置文件很明显是不合适的(这种情况下，系统将自动选择限制最严格的配置文件)，会使得所需的功能受到影响。

还有一个更常见的例子。例如，有人正在使用笔记本电脑通过咖啡馆的无线网络上网浏览网页，但同时需要使用 VPN 拨号访问公司网络中的共享资源。在这种情况下，等于有了 WiFi 和 VPN 两个网络连接，分别用于不同的用途。但在 Windows 7 之前，系统将对这两个连接应用针对公用网络的配置文件，禁用网络发现以及资源共享等功能。虽然安全性得到了保障，但通过 VPN 连接访问公司共享资源的做法将无法实现。

因此，在 Windows 7 中，如果有多个可用的网络连接，那么系统会分别针对每个连接的类型，同时使用多个防火墙配置文件。这样不同的网络可以受到不同的保护，既可以保证安全性，也可以保证易用性。

通常，Windows 防火墙工作在后台，并不会对我们的正常使用产生太多干扰。但有些时候，可能需要将该防火墙禁用，例如安装了其他防火墙，但 Windows 没能正确识别，导致同时运行了两个防火墙；或者网络遇到问题，需要禁用防火墙，并对问题进行排查。此时，只要直接在图 8-1 所示的界面中单击左侧的“打开或关闭 Windows 防火墙”链接，随后将看到图 8-2 所示的界面。

在这里可以根据不同的类型决定 Windows 防火墙的行为。例如，我们可以在专用网络

上关闭 Windows 防火墙，只在公用网络中打开；或者也可以直接设置在公用网络上阻止所有传入的连接。当然，如果确实有必要，也可以通过“关闭 Windows 防火墙”选项，针对某个网络类型禁用 Windows 防火墙。设置完毕后单击“确定”按钮即可。

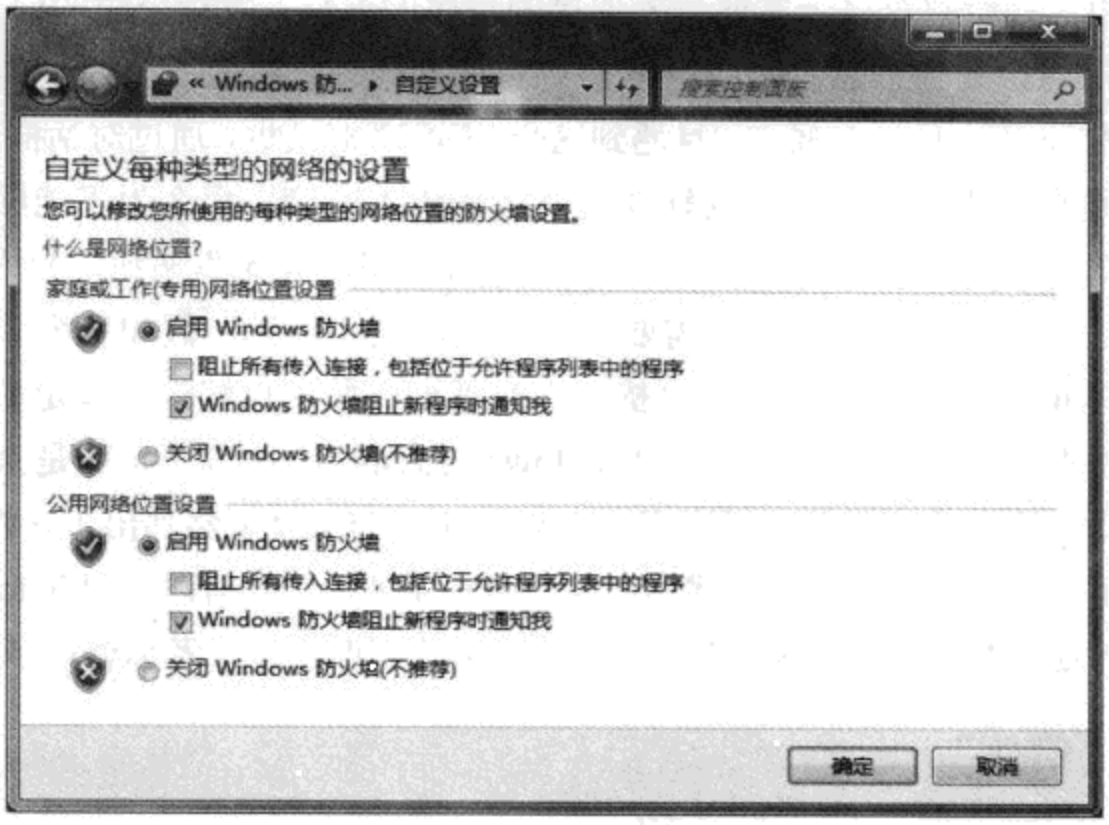


图 8-2　针对不同的网络类型对防火墙进行配置

图 8-2 所示的“传入连接”是什么意思？举例来说，在使用某些程序（一般多见于实现文件传输的程序，例如 P2P 下载软件、语音视频聊天软件等）时，一旦这些程序需要接受传入连接，那么 Windows 防火墙会使用图 8-3 所示的对话框提醒用户注意。

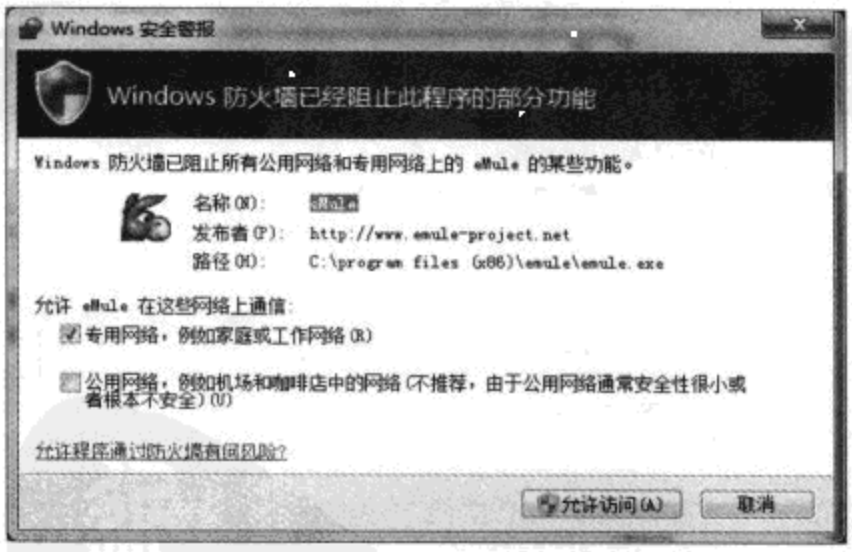


图 8-3　遇到未经请求的传入连接后，防火墙会询问是否允许

这意味着为了实现程序所需的功能，需要主动接受来自外界的数据包，也就是“传入连接”，而这与通常情况下的“传出”网络通信是完全不同的。因为通常情况下，必须首先由客户端发起通信，例如要浏览网页，必须由客户端的浏览器主动联系 Web 服务器，服务器才能知道我们要浏览的页面地址，这种本机主动发起的通信不会受到 Windows 防火墙的

限制。但在进行传入通信的过程中，相关的连接并非是本机请求的，而是外界主动发送的，虽然很多正常的程序需要这样做，但大部分病毒、蠕虫、网络攻击等危险因素也需要这样做，因此，Windows 防火墙会对未经主动请求的传入连接进行限制。

在图 8-3 中，一般都会显示需要传入连接的程序的名称、发行公司的信息、安装路径，以及要访问的网络位置等信息，通过这些信息可以判断该连接是否是我们需要的。例如，在使用 P2P 软件下载文件的时候，一旦遇到这个“提示”对话框，通过对话框中提供的信息，我们已经知道是自己正在使用的下载软件需要接受传入连接，那么为了能够让软件正常工作，自然需要选择相应的防火墙配置文件，然后单击“解除锁定”按钮，允许在所选配置文件上接受传入连接。这个工作通常只需要进行一次，也就是说，假如某个软件需要接受传入连接，那么 Windows 防火墙显示了“提示”对话框，并且也解除了锁定后，下次运行该软件，如果软件依然需要接受传入连接，Windows 防火墙将不再提示，而是直接 . 允许。

另一种情况，如果没有运行新的程序，但 Windows 防火墙突然弹出了这样的对话框，并且显示的程序信息都是很陌生的（程序信息这一点很重要，因为有时候 Windows 自身的某些功能也需要传入连接），很明显，这可能是系统中的某些间谍软件或者恶意程序需要访问网络。

8.1.2 使用“例外”

上文中说到的 Windows 防火墙允许程序的传入连接的例子，实际上，在“Windows 防火墙设置”对话框中还有更详细的设置。在 Windows 防火墙主界面上单击左侧的“允许程序或功能通过 Windows 防火墙”链接，随后可以看到图 8-4 所示的界面。其实上文中所谓的被允许的传入连接就是 Windows 防火墙中的例外，而除了指定的传入连接外，其他所有的传入连接都是直接被拒绝的。

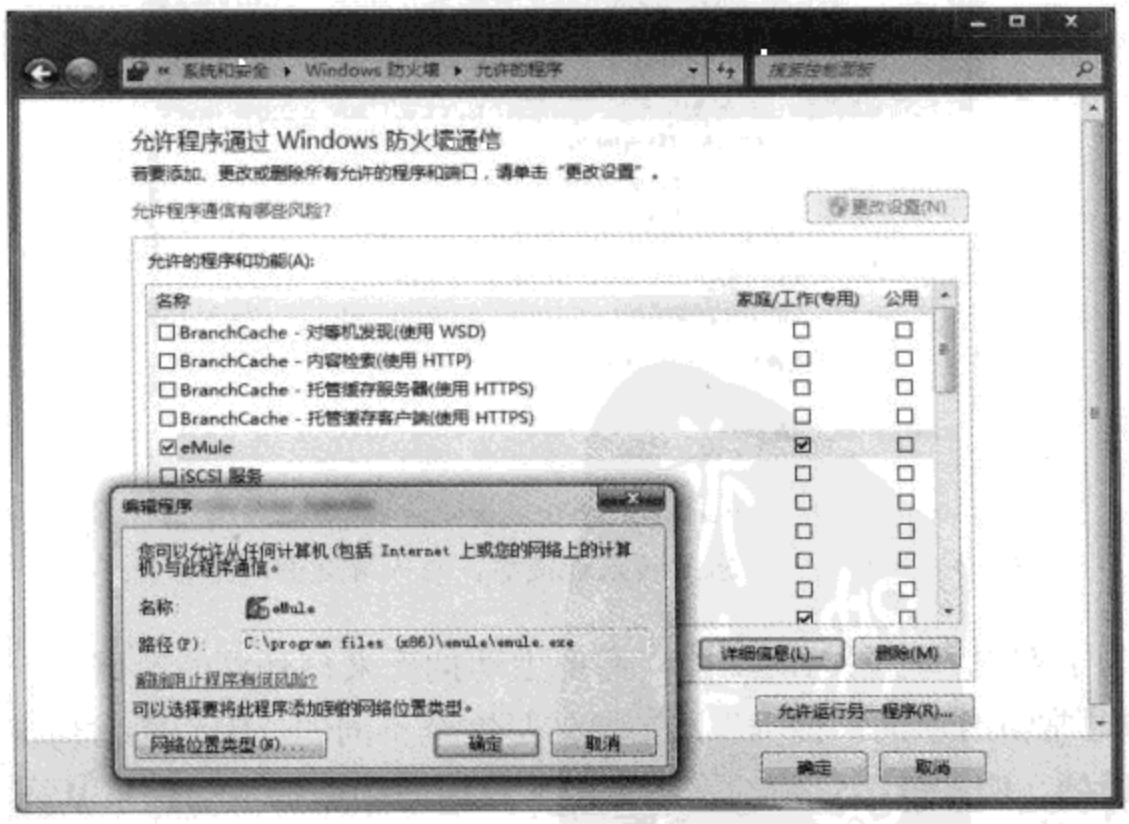


图 8-4 管理和添加防火墙例外

在程序列表中可能会显示很多内容，这些内容都是和计算机上安装的程序有关的。不仅如此，这里还有一些 Windows 自带的内容，对于这类内容，建议不要随便更改设置，以免影响 Windows 的正常功能。

对于显示的所有例外项目，有些在名称前面有对勾，有些没有，对勾表示该例外是被启用的，而没有的表明该例外只是被创建，但没有启用。同时，这也是一种安全措施，一般情况下，对于那些偶尔使用，但是需要接收传入连接的程序，可以在不需要使用的时候将对应的例外条目禁用，需要使用的时候再打开。这样也可以防范攻击者利用一些流行程序的固定端口发起攻击。

单击选中一条例外条目，并单击“详细信息”按钮，可以打开图 8-4 左下角所示的“编辑程序”对话框，在这里可以查看该条目对应程序名称和安装路径等信息，同时还可以查看该条目适用的配置文件。如果确信自己不再需要某个例外条目，也可以单击将其选中，然后单击“删除”按钮将其彻底删除。

为了方便使用，还可以在运行一个程序之前就创建好对应的例外条目，不过这要求对该程序的一些网络参数有所了解，因此，只建议熟练的用户使用。

如果需要为某个特定的程序创建例外，可以采取添加程序的方式进行。如果要使用这种方式，我们必须了解目标程序需要访问的网络范围。通过程序创建例外的具体过程如下：

STEP 01 在图 8-4 所示的界面上单击“允许运行另一程序”按钮，随后会打开“添加程序”对话框，该对话框列出了系统中已经安装的全部程序。

STEP 02 单击选中目标程序，所选程序的安装路径会显示在程序列表下方的“路径”文本框中。如果需要使用的程序没有列出来，也可以单击“浏览”按钮，使用随后出现的“浏览”对话框定位程序，在这里主要是选择程序的主文件，通常是.exe 文件。

STEP 03 确定了要创建例外的程序后，还需要为规则决定应用到的配置文件。也就是说，该规则是应用于公用网络、专用网络，还是两种网络都应用。这时候可以单击“网络位置类型”按钮，随后可以看到图 8-5 所示的“选择网络位置类型”对话框。

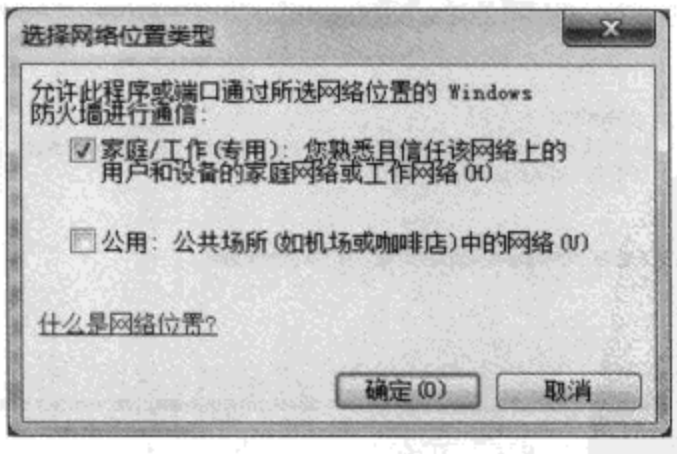


图 8-5　选择该例外应用到的配置文件

STEP 04 在选择网络位置类型的时候需要注意，只有在连接到规则应用到类型的网络后，该规则才会生效。也就是说，如果这个规则只应用于公用网络，那么在专用网络中，

规则依然是被禁用的。

STEP 05 设定好应用范围后，单击“添加”按钮即可。

8.1.3 网络位置

上文曾多次提到网络位置以及网络类型等概念，下面将详细介绍它。

很多人可能经常会遇到这样的情况：自己有一台笔记本电脑，在公司里需要通过网线连接到公司的网络中，因为公司网络已经做好了充分的保护，同时为了工作需要，必须在公司网络中共享自己计算机上的文件，访问别人的共享，或者使用共享打印机。然而在出差时，可能需要使用同一台笔记本在机场使用无线网络上网，收发邮件，因为机场网络对于我们来说，是“不被信任”的，因此，为了安全起见，可能要关掉文件共享，同时提高防火墙的安全级别，保护自己系统的安全。

对于熟练用户来说，上面这些操作只是麻烦一点，但至少还是可以做到的。但对于不熟练的人，或者只是用计算机工作，而对这方面没有多少了解的人来说，让他根据网络的实际情况调整安全设置几乎是不可能的。为了解决这种问题，微软从 Windows Vista 开始提供了一种叫做“网络位置”的功能。

简单地说，当我们第一次将系统连接到某个网络后，系统首先会弹出图 8-6 所示的对话框，让我们选择网络位置。

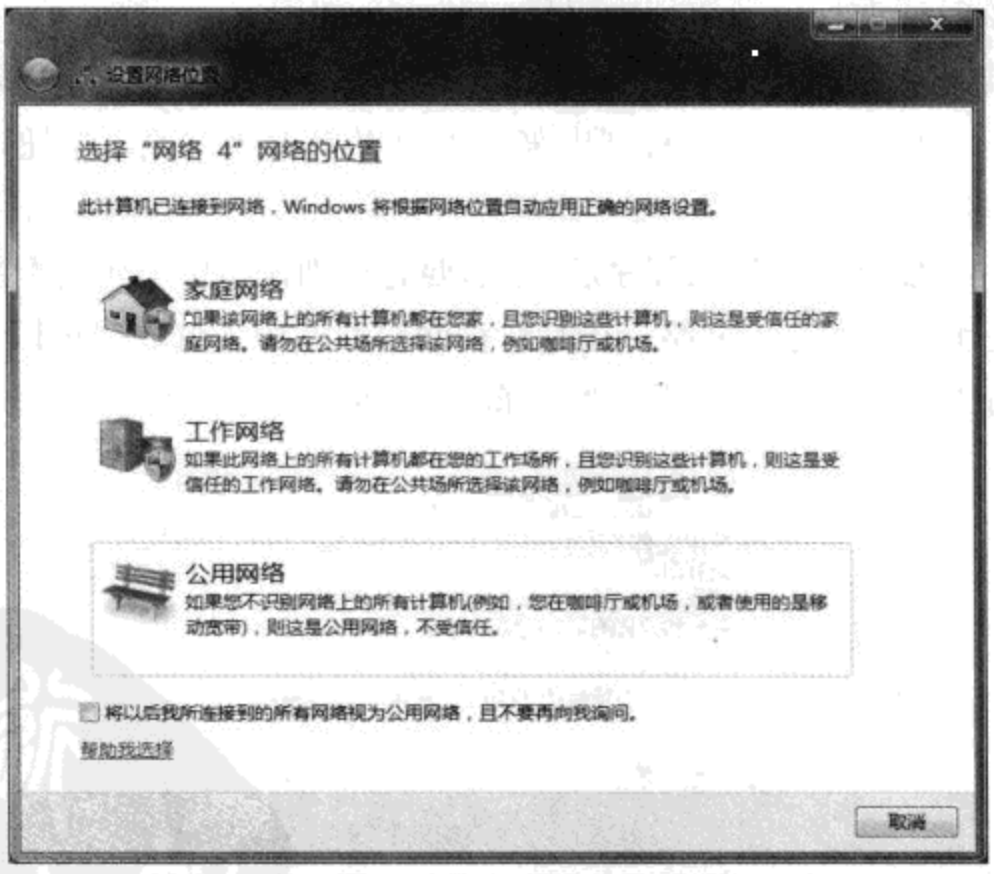


图 8-6 正确选择新网络的类型

Windows 将网络分为三种类型：公用网络、专用网络，以及域网络（域网络只有在计算机加入域后才能使用，本书不过多讨论）。在图 8-6 所示的界面中，需要根据实际情况选

择正确的网络类型。举例来说，如果选择“家庭”或“工作”，那么 Windows 会将这个网络识别为专用网络。专用网络属于可信任网络，因此，Windows 防火墙的安全级别会低一些，同时 Windows 会自动在这个网络上启用网络共享和发现、打印机和文件共享等局域网中常用的服务。

如果选择“公用网络”，Windows 会将这个网络识别为公用网络。公用网络属于不可信任网络，因此，Windows 防火墙的安全级别会相当高，不仅如此，这种网络上的各种非必要的服务都会被禁用，以便能增强安全性。在选择这种网络位置后，将看不到同一局域网的其他计算机，当然对方也看不到我们。另外，如果只有一台计算机，没有局域网环境，为了安全起见，也建议选择这种网络类型。

这里有一个很体贴的设计，当为网络选择了适当的类型后，Windows 会将相应的配置信息保存起来，这样，下一次连接到同一个网络的时候就不会询问，而是根据上次的设置直接应用相应的选项。

很多人都在这上面遇到一些问题，例如系统装好了，可不知怎么回事，就是看不到局域网中其他计算机上的共享文件，别人也看不到自己机器上的共享文件。这时候应该考虑是不是第一次连接到这个网络时选择了错误的网络位置，因为一旦错误地将专用网络设置为了公用网络，那么网络上的一些活动就会受到影响。这时候我们可以考虑修改网络位置设置，方法如下：

STEP 01 在屏幕右下角的系统通知区域找到代表网络连接的图标，单击该图标，从弹出的菜单中单击“打开网络和共享中心”链接。

STEP 02 单击要管理的网络名称下方对应的链接（如图 8-7 所示），例如，如果希望修改“网络 4”的网络位置，以及其他相关设置，单击图中对应“网络 4”的“xx 网络”链接。

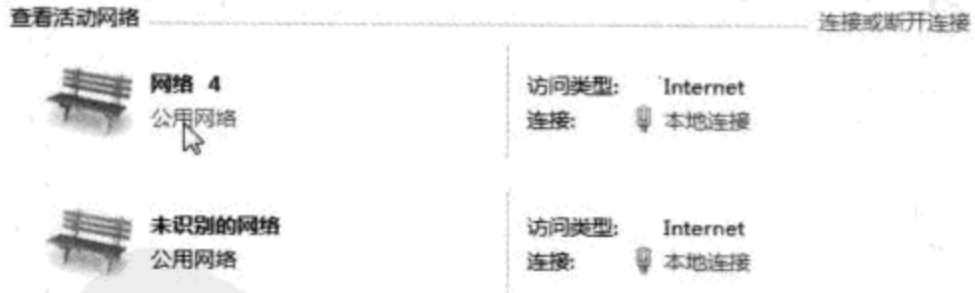


图 8-7　查看活动的网络

STEP 03 随后会重新看到类似图 8-6 所示的对话框，在这里可以根据实际情况选择不同的网络位置。

如果计算机曾连接过多个不同的网络，那么为了能够准确地区分，还可以给不同的网络选择一个不同的图标，此时可以单击图 8-7 中每个网络名称左侧的图标，这将打开设置网络属性对话框，在该对话框中，可以通过“网络名”文本框为这个网络设置一个更友好

的名称，例如“xxx 家的无线网络”。另外，还可以单击“更改”按钮，为该网络指定一个不同的图标，例如，“xxx 的大头照”或者公司的徽标。

8.2 高级安全 Windows 防火墙

Windows 防火墙最被人诟病的一点就是功能太简陋，主要是无法控制本机程序对网络的主动访问。而且 Windows 防火墙的配置比较麻烦，大部分选项都必须在图形界面下进行配置，这在企业网络中是很麻烦的。

为了解决这些问题，从 Windows Vista 开始，微软还提供了高级安全 Windows 防火墙，这个防火墙主要针对企业网络，因此，完全是以组策略的形式存在，方便管理员集中配置和管理。只不过该防火墙的设置有些烦琐，不像第三方防火墙那么友好。

对于计算机水平一般，且不打算深入学习，但又不满足于 Windows 防火墙的简单功能的读者，建议安装更友好的第三方网络防火墙软件。如果对计算机技术比较了解，或者需要通过网络集中管理多台计算机的防火墙设置，推荐使用高级安全 Windows 防火墙。使用高级安全 Windows 防火墙并不需要禁用 Windows 防火墙。

有很多方法可以打开高级安全 Windows 防火墙的配置界面，例如运行“secpol.msc”，打开本地安全策略控制台，然后从控制台窗口左侧的控制台树中依次进入到“安全设置”→“高级安全 Windows 防火墙”节点。这样做很麻烦，我们也可以直接运行“wf.msc”，打开高级安全 Windows 防火墙的设置界面（如图 8-8 所示）。

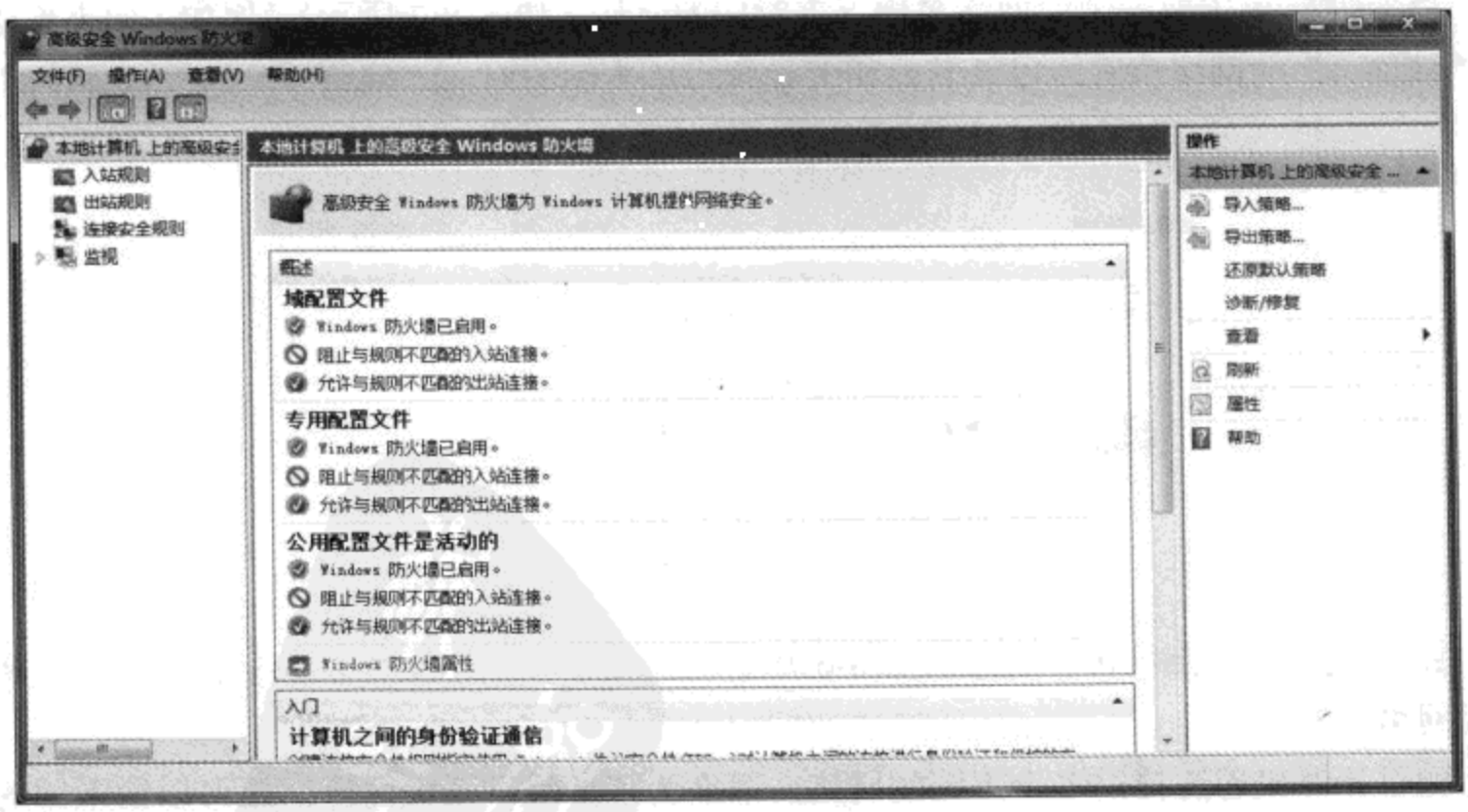


图 8-8 高级安全 Windows 防火墙的主窗口

下面首先介绍一下这个界面上的每个元素。

在左侧的控制台树中有很多子节点，这些子节点分别可以查看和修改高级安全 Windows 防火墙的各项功能。“入站规则”节点下可以看到所有控制传入连接的规则；“出站规则”节点下可以看到所有控制传出连接的规则。而控制传出连接是高级安全 Windows 防火墙和 Windows 防火墙的最主要区别，同时也是很多人期待已久的功能；“连接安全规则”节点下可以看到所有和 IPSec 有关的规则；“监视”节点下可以看到高级安全 Windows 防火墙的各种工作状态。

随后，中央的窗格中显示了高级安全 Windows 防火墙的主要内容，随着在左侧的控制台树中选择不同的子节点，中央窗格中就会显示出对应的内容。

右侧的操作窗格则列出了当前选中的与节点有关的操作，随着选择的子节点的不同，这里提供的操作会有所变化。同时，操作窗格中显示的大部分选项还可以在子节点上单击鼠标右键后从右键菜单中看到。

考虑到本书的适用范围，这里只打算介绍在单机和工作组环境下高级安全 Windows 防火墙的使用。实际上，在域环境下，高级安全 Windows 防火墙的集中管理的功能才能最大程度地发挥出来，不过域环境并不在本书的讨论中。

在左侧控制台树中的“本地计算机上的高级安全 Windows 防火墙”节点上单击鼠标右键，选择“属性”，可以打开图 8-9 所示的“高级安全 Windows 防火墙属性”对话框，在这里可以针对高级安全 Windows 防火墙的一些常规选项进行设置。

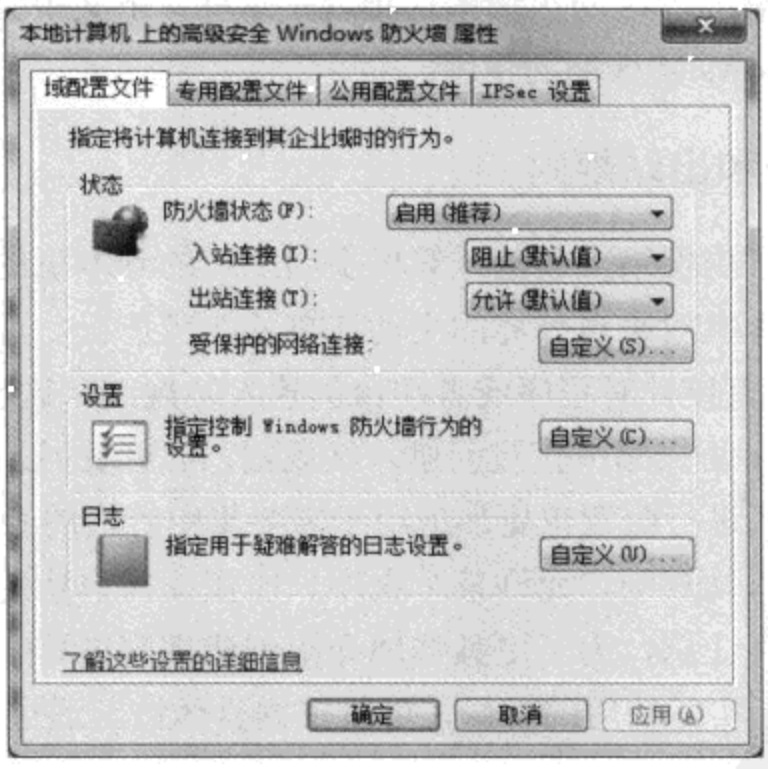


图 8-9 “高级安全 Windows 防火墙属性”对话框

首先，请注意该对话框提供的选项卡，每个选项卡对应了不同配置文件下的设置，因此，如果要调整高级安全 Windows 防火墙的选项，请先打开目标配置文件对应的选项卡。例如，在单机和工作组环境下，可以分别针对专用网络和公用网络在专用配置文件和公用配置文件选项卡下进行配置。

对于前三个对应了不同配置文件的选项卡，其中的内容都是一样的，例如可以使用防火墙状态下拉菜单决定是否在当前配置文件中启用高级安全 Windows 防火墙，同时可以在入站连接和出站连接下拉菜单中选择对于不同类型的连接将会采取什么样的措施，可选的选项包括：

- **阻止** 该选项将会阻止没有被列在例外列表中的所有符合条件的连接。
- **阻止所有连接** 该选项将会阻止所有符合条件的连接，并且不考虑例外列表的内容（该选项仅适用于入站连接）。
- **允许** 该选项将允许所有符合条件的连接。

单击“设置”选项下的“自定义”按钮后，可以打开自定义配置文件的“设置”对话框，在这个对话框中可以设置一些高级选项。例如，通过“显示通知”下拉菜单可以决定在防火墙阻止了入站连接后是否向用户发出通知；“允许单播响应”下拉菜单决定了是否允许本机接收来自其他计算机的单播响应，一般情况下，没必要调整该选项的设置。

单击“日志”选项下的“自定义”按钮后，可以打开自定义配置文件的“日志设置”对话框，在这里我们可以指定日志文件的保存位置、日志文件大小上限，以及日志文件的记录内容等信息。

IPSec 设置选项卡下的内容用于控制 IPSec，该功能对于一般用户没什么用处，因此，本书不准备过多涉及。

基本上，高级安全 Windows 防火墙的选项就是这些，下文中会针对一般用户最常见的需要介绍高级安全 Windows 防火墙的使用。

8.2.1 创建入站规则和出站规则

入站规则主要控制了由网络上其他计算机主动发起的到本机的连接。通过创建入站规则，可以更有效地控制本机对来自外界的主动连接的响应情况。注意，对于一般用户，通过 8.1.2 节中介绍的方法直接针对程序或者端口创建入站规则，这也是一种更简单的方法。不过在高级安全 Windows 防火墙中直接创建入站规则，其规则的设置可以更加复杂和强大，当然，通过组策略的形式进行配置也更加适用于需要集中管理的企业环境。

假设需要创建一个入站规则，允许某个程序只能接受来自特定网络地址的入站连接，可以按照下列步骤操作（注意，为了更具体地介绍创建规则过程中的一些选项，下面的操作使用了最复杂的步骤，实际使用的时候，可以根据具体情况通过选择 Windows 提供的现成选项简化操作）：

STEP 01 在“入站规则”节点上单击鼠标左键，将其激活，然后单击鼠标右键，选择“新建规则”，随后可以打开如图 8-10 所示的“新建入站规则向导”。

STEP 02 在这里可以创建 4 种不同类型的入站规则，这 4 种类型的规则用途分别如下：

- **程序** 该选项可以为特定的程序创建入站规则。

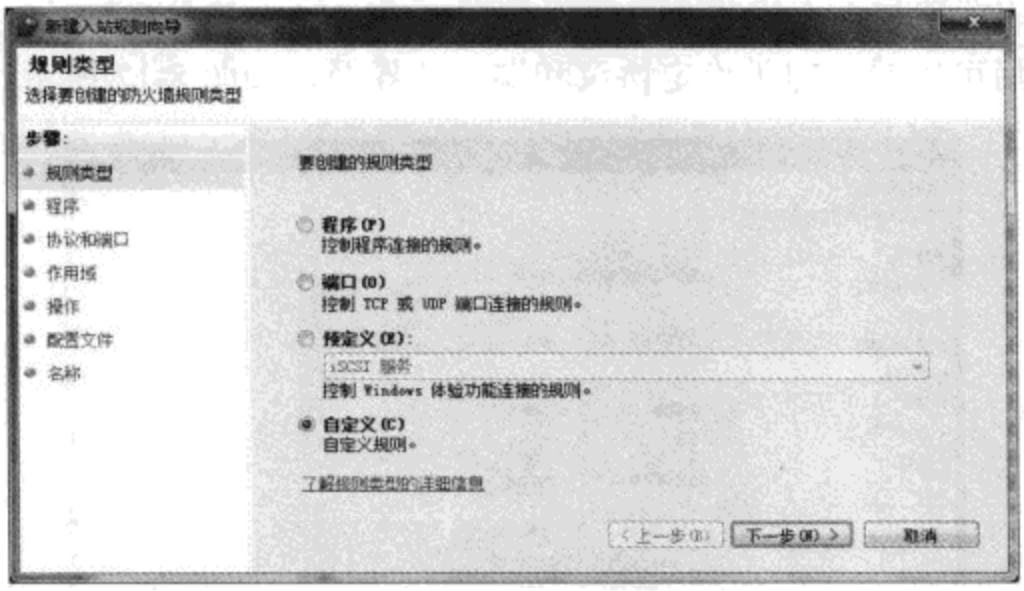


图 8-10　通过该向导可创建入站规则

- **端口**　该选项可以为特定的端口创建入站规则。
- **预定义**　该选项可以为一些预置的服务创建入站规则，选择该选项后，可以从下拉菜单中选择该规则适用的服务。
- **自定义**　该选项可以完全按照我们的需要创建出最合适的规则。当然，选择该选项后，接下来需要配置的选项也是最多的。

如果不知道自己需要创建哪种规则，请单击向导窗口下方的“了解规则类型的详细信息”链接，查看 Windows 提供的帮助。

在这里选择“自定义”，然后单击“下一步”按钮。

STEP 03　随后需要选择该规则适用的对象，可用的选项包括“所有程序”和“此程序路径”，因为需要针对特定程序使用该规则，因此，选择“此程序路径”选项，然后在下方的文本框中输入程序的完整路径（也可以单击“浏览”按钮定位程序）。

如果这个规则是为某个服务创建的，那么可以直接单击“自定义”按钮，并在随后出现的自定义服务设置对话框中选择目标服务（如图 8-11 所示）。

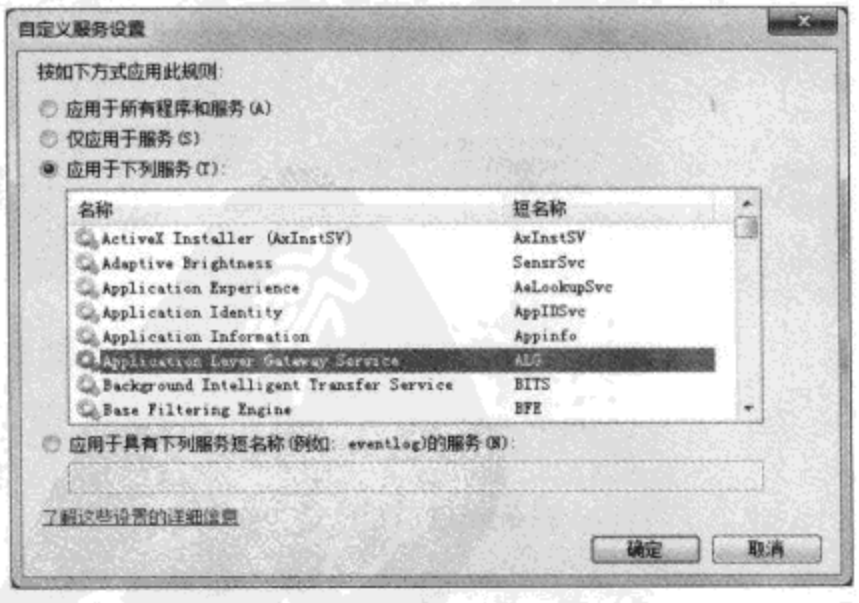


图 8-11　选择该规则应用给的服务

设置好所有的选项后，单击“下一步”按钮。

STEP 04 随后可以看到用于设定协议和端口的界面，如图 8-12 所示。

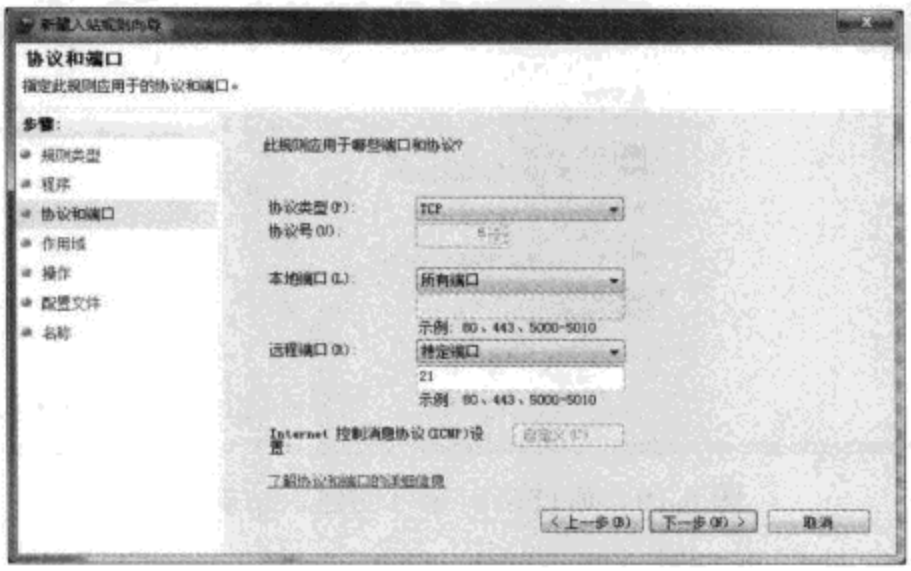


图 8-12　确定该规则的适用协议和端口

首先在“协议类型”下拉菜单中选择该规则需要对应的协议类型，阅读过上文后就应该记得，在 Windows 防火墙中，可选的类型只有 TCP 和 UDP 两种，然而在高级安全 Windows 防火墙中，支持的协议类型达到了 15 种之多。随着选择不同的协议类型，下方的“协议号”文本框中就会显示当期所选协议类型对应的协议号。如果需要使用的协议没有列出来，也可以在“协议类型”下拉菜单中选择“自定义”，然后手工输入需要的协议所对应的协议号。

接下来还需要设置本地端口和远程端口，“本地端口”下拉菜单下提供的选项较多，共有 5 种，我们可以根据实际需要进行选择，或者选择“特定端口”，然后在下方的文本框中输入端口号。如果在上方的“协议类型”下拉菜单中选择了和 ICMP 有关的协议，那么还可以单击“自定义”按钮对 UCMP 数据包的限制进行更进一步的设定。

设置好所有的选项后，单击“下一步”按钮。

STEP 05 接下来需要设置该规则适用的网络范围，此时可以看到图 8-13 所示的界面。

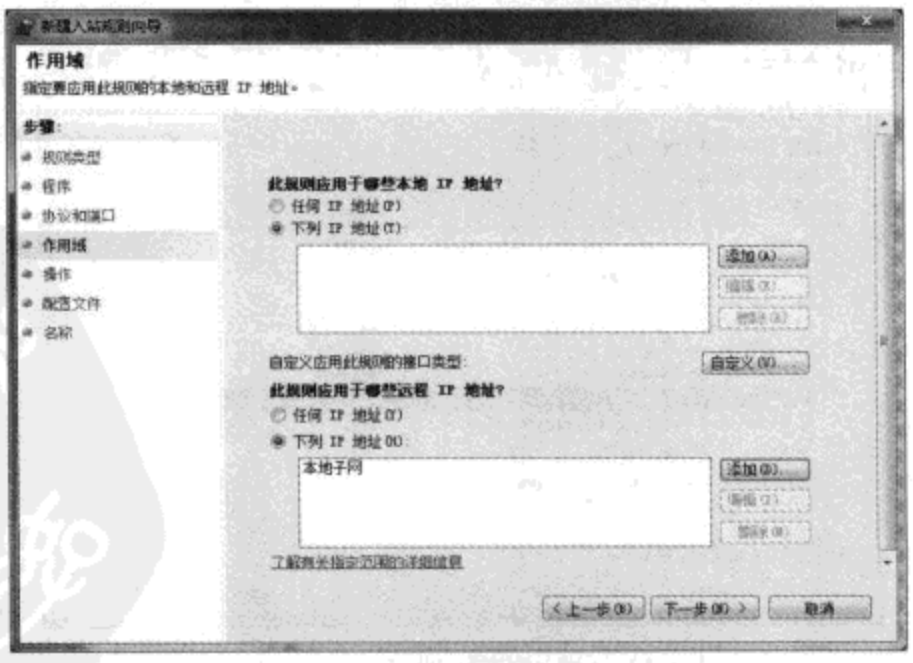


图 8-13　设定规则的适用范围

在“此规则应用于哪些本地 IP 地址”选项下，可以指定对哪些本地地址范围应用该规则，单击“添加”按钮后可以添加地址。在添加的时候，可以指定某个特定的 IP 地址、某个 IP 地址段或者 IP 地址范围。

如果需要决定该规则可以适用于哪些类型接口的网络连接，则可单击“自定义”按钮进行选择。例如，我们可能会使用无线网卡连接到不同的网络中，那么就可以让这个规则应用给使用本机的无线网卡访问到的所有网络。

在“此规则应用于哪些远程 IP 地址”选项下，可以指定对哪些远程地址范围应用该规则，单击“添加”按钮后可以添加地址，同时在添加地址的时候，可以像添加本地 IP 地址那样使用完全一样的选项来添加。

在设置远程地址时，还可以通过某些规则批量选择应用给的计算机。例如，如图 8-14 所示的就是添加远程 IP 地址的对话框，在这里可以通过“预定义计算机集”下拉菜单将该规则应用给所有符合同一条件的所有计算机，例如，所有使用同一个 DHCP 服务器的计算机。

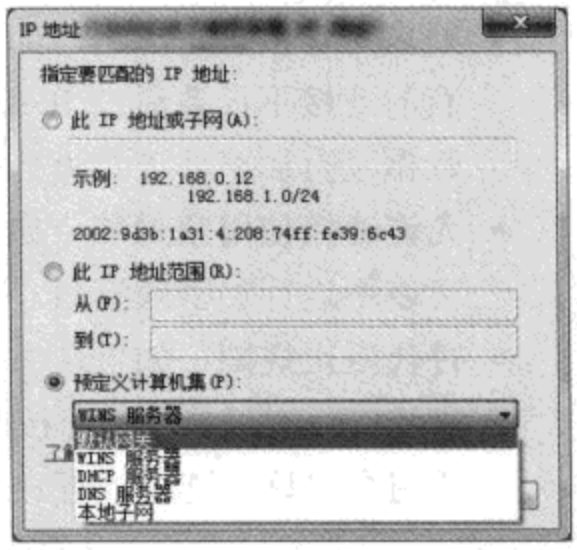


图 8-14　通过规则指定一批计算机

设置好之后，再次单击“下一步”按钮。

STEP 06 接下来要设置的是连接类型，此时可以看到如图 8-15 所示的界面。

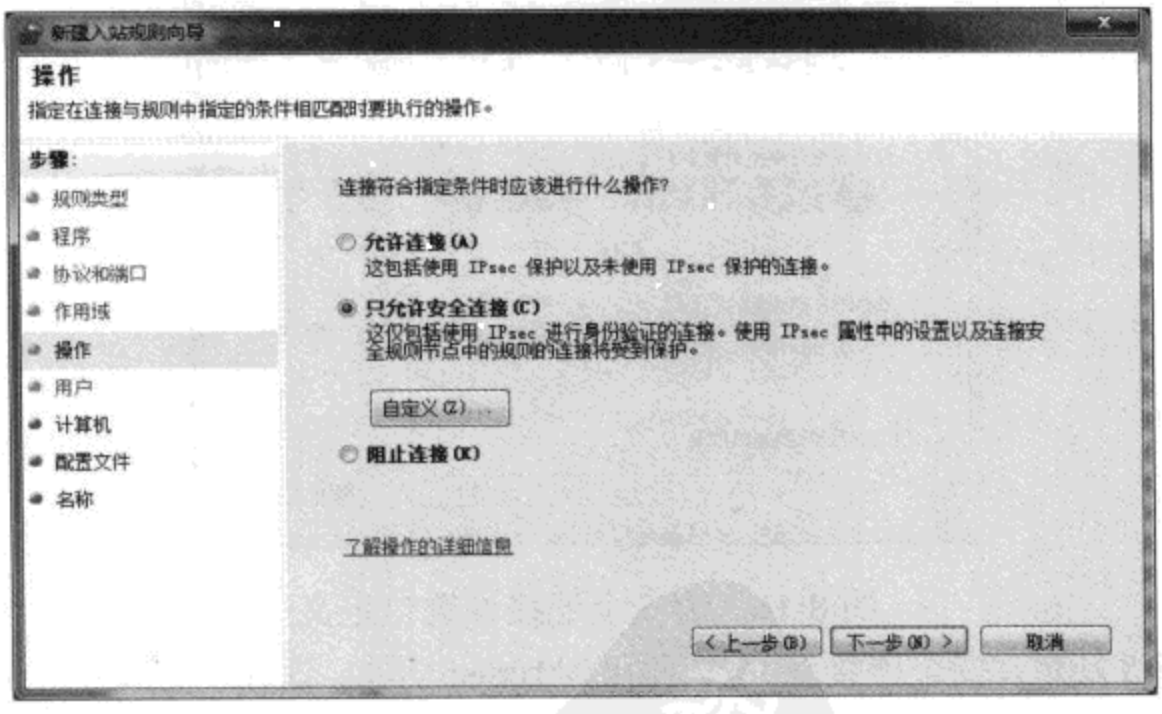


图 8-15　设定该规则允许的连接类型

在这里可以决定，对于符合上面设置过条件的连接采取怎样的操作，如果希望允许符合上述条件的连接，可以在这里选择“允许连接”或“只允许安全连接”；如果希望阻止符合上述规则的连接，可以选择“阻止连接”。

如果决定允许连接，通过选择“只允许安全连接”选项，还可以进一步限制允许连接

的类型，例如选择该选项后，只有使用 IPSec 进行过身份验证，以及完整性保护的连接才会被允许。不仅如此，还可以通过“自定义”按钮对允许的安全连接进行更进一步的限制。单击“自定义”按钮后，可以看到如图 8-16 所示的界面，这里提供的选项和作用如下：

- **仅允许通过身份验证和完整性保护的连接** 如果选中该选项，则只有使用 IPSec 进行了身份验证的计算机才能进行连接，老版本 Windows 不支持这一方式。
- **要求对连接进行加密** 如果选中该选项，那么高级安全 Windows 防火墙将会要求所有的连接不仅要通过 IPSec 进行身份验证，同时还要对传输的数据进行加密。如果数据没有加密，连接就会被拒绝。
- **允许连接使用空封装** 如果选中该选项，则允许的连接只需要进行身份验证即可，可以不进行加密或签名。
- **替代阻止规则** 如果选中该选项，假设有一个连接，如果按照选中了这个选项的规则已经可以通过了，而按照其他规则不能通过，那么最终的高级安全 Windows 防火墙将会对这个连接放行。

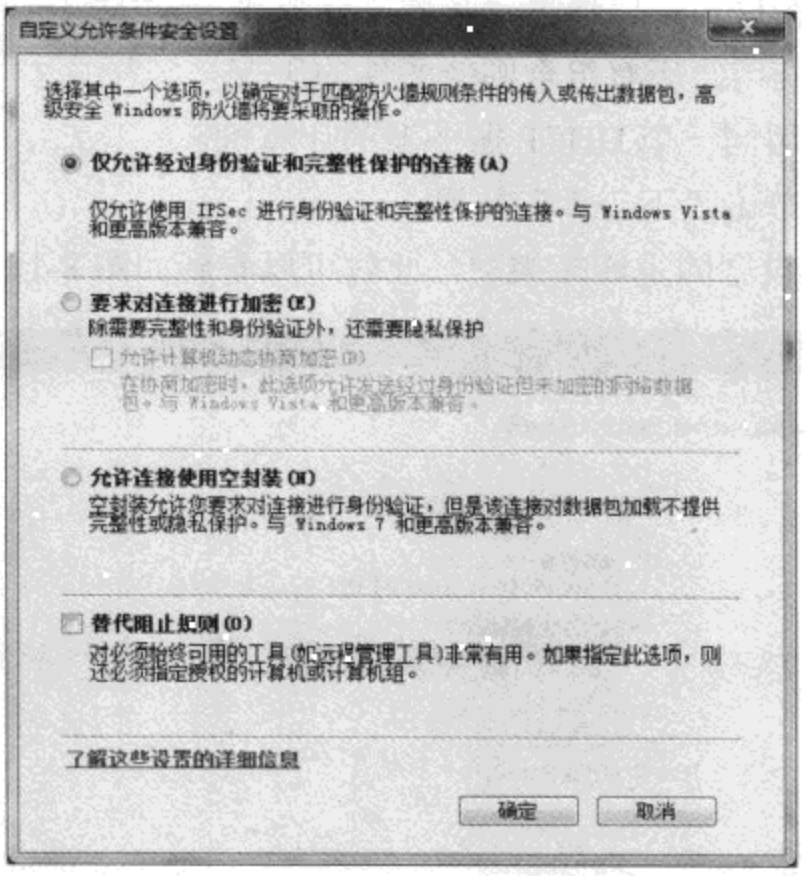


图 8-16 为安全连接设置自定义条件

如果选择“只允许安全连接”，那么将用到 IPSec 功能，这在单机或工作组环境下并不实用。因此，可以直接选择“允许连接”或“阻止连接”，然后单击“下一步”按钮继续。

STEP 07 接下来需要选择该规则应用的范围，可供选择的选项有“域”、“专用”，以及“公用”，简单来说，该选项决定了这条策略会被应用到哪个配置文件中，也就是说，通过该规则，我们可以决定哪些类型的网络将会被应用该规则。因此，我们可以根据实际情况来选择。

STEP 08 为这个规则输入一个名称和描述，这里建议输入一些具有一定含义的内容，至少要能通过规则的名称知道这条规则的用途，并能够通过描述知道有关该规则的一些大致信息。输入完成之后，单击“完成”按钮即可。

出站规则的创建步骤和入站规则的创建几乎完全一致，只不过，出站规则影响的是对外的主动连接。因此，详细的过程在此省略。

8.2.2　查看和管理规则

随着不同规则的创建，高级安全 Windows 防火墙中可能会产生很多新的规则，在规则数量多到一定程度后，相互之间可能会产生冲突，或者带来安全隐患。因此，定期对规则进行管理也是保证系统安全的一个重要手段。高级安全 Windows 防火墙中的很多功能都为规则的管理提供了方便。

1．规则的处理

创建好一个规则后，该规则立刻就会被启用，此时，我们可以单击“入站规则”、“出站规则”和“连接安全规则”节点，直接查看相应的规则。例如，在进入某个节点后，可以看到图 8-17 所示的内容。

图 8-17　查看和管理不同的规则

首先要注意的是，在 Windows 7 中，默认情况下，就已经有很多系统预置的防火墙规则了，对于这些规则，一般情况下不建议自己调整或者删除，因为有可能会影响到系统功能的正常使用。

同时，所有规则的名称前面会看到绿色或灰色的图标，绿色表示该规则目前被启用，灰色表示该规则目前被禁用。在窗口右侧的操作窗格中，随着单击选中一个规则后，就会出现相应的操作选项供我们直接单击使用。

如果觉得这里显示的规则太多，不便于管理，还可以使用筛选功能。在右侧操作窗格的顶部有“按配置文件筛选”、“按状态筛选”以及“按组筛选”三个选项，单击这三个选项中的任何一个之后，就会弹出一个菜单，通常，菜单上的选项取决于具体的菜单内容。例如单击“按配置文件筛选”后，弹出菜单中就会列出三种不同的配置文件供我们选择。这些筛选条件还可以叠加，例如可以首先按照配置文件筛选，然后按照状态筛选，最后按照组筛选。相信通过合理地利用筛选功能，很快将能在众多规则中找到自己需要的。

如果需要编辑一个现有的规则，可以单击选中目标规则，然后单击右侧操作窗格中的“属性”链接，随后会打开该规则的“属性”对话框，我们可以在这个对话框中调整相应的属性。再次提醒，不建议编辑系统预设的规则。对于系统预设的规则，在“规则”属性对话框的“常规”选项卡顶部还会显示比较明显的提示信息，用于提醒我们注意。

2. 导入和导出规则

在域环境下，管理员通过活动目录可以将高级安全 Windows 防火墙的设置批量应用给多台计算机。在单机或工作组环境下，难道我们就只能一台一台地手工设置吗？当然不是，高级安全 Windows 防火墙为我们提供了导入和导出功能。

在一台模板计算机上创建并配置好所有的规则后，用鼠标右键单击“本地计算机上的高级安全 Windows 防火墙”节点，从右键菜单中选择“导出策略”，随后将看到“另存为”对话框。在“另存为”对话框中为导出后的文件选择一个保存位置以及文件名，并单击“保存”按钮即可（注意，在选择保存位置的时候，请保持“保存类型”下拉菜单中默认选中的文件类型不变）。

随后将导出的.wfw 文件复制到其他所有需要应用同样防火墙设置的计算机上，运行 wf.msc，打开高级安全 Windows 防火墙的配置界面，并在“本地计算机上的高级安全 Windows 防火墙”节点上单击鼠标右键，选择“导入策略”，Windows 会提醒我们这样做会使本机当前的所有防火墙策略都被覆盖，并询问是否继续。选择“是”按钮，在随后出现的“打开”对话框中选中复制过来的.wfw 打开即可。

在导入了来自其他计算机上的策略后，请对被导入的计算机进行仔细的测试，主要是看平时需要使用的程序是否会受到不利的影响。同时，为了便于恢复，在将其他计算机上的设置导入本机之前，最好将本机的设置先导出并备份，这样，一旦导入的设置出现了问题，利用之前的备份还可以轻松地还原。

8.3 配置网络列表管理器策略

上文曾经简单介绍过有关网络位置功能的使用。实际上，为了方便管理员对所有计算

机的不同网络位置所用的防火墙配置文件进行统一的配置和管理，在 Windows 7 中还提供了网络列表管理器策略。

要使用这些策略，请运行“secpol.msc”，打开本地安全策略控制台，并在左侧树形图中单击“网络列表管理器策略”，随后，相关内容就会显示在右侧窗格中（如图 8-18 所示）。

对于这些策略，主要目的就是为了针对不同类型的网络设置要使用的防火墙配置文件，并决定是否允许最终用户修改这些文件。在该策略节点下，可以通过“无法识别的网络”、“正在识别网络”以及“所有网络”这三个节点决定对于计算机加入的其他网络采取怎样的配置。同时，计算机目前已经连接到的网络也会显示在这里，例如，图 8-18 中的“MyNet”就是这台计算机已经连接的网络。

对于工作组环境的普通用户，这些策略主要可用于这样一种情况：某些情况下，如果连接到某些陌生的网络，因为某种原因，可能导致网络无法被正确识别，甚至 Windows 可能根本不会询问该网络的位置类型。这种网络被 Windows 称为“无法识别的网络”，而这样的网络可能根本无法正常使用，或者会遇到其他奇怪的问题。

如果遇到这样的情况，可在图 8-18 所示的界面中双击“无法识别的网络”，打开图 8-19 所示的属性对话框，并为所有的此类网络中手工指定要使用的防火墙配置文件（为了安全起见，建议使用“公用”）。

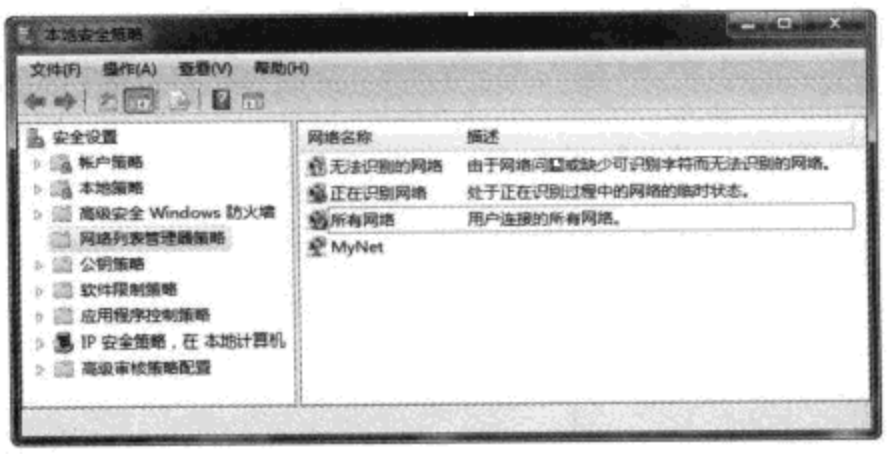


图 8-18　网络位置的相关内容也可通过策略进行设置

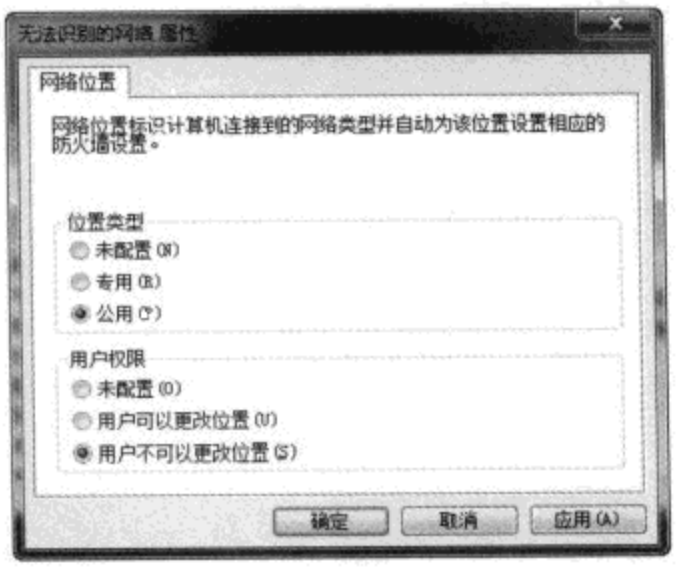


图 8-19　对无法识别的网络集中选择防火墙配置文件

在“用户权限”选项下，可以决定普通用户是否允许更改此类网络的位置。由于这类网络通常都是不可信任的，而且我们已经指定了使用公用配置文件，因此，通常建议禁止用户更改此类网络的位置，以免危害到本机的安全性。

同时需要注意，这些修改将影响到所有符合条件的网络，例如在本例中，经过上述修改，以后连接的每一个无法正确识别的网络都会应用相同的防火墙设置。因此，为了获得最大程度的安全，修改这些内容的时间以“安全第一”为主，不要为了贪图一时的方便而威胁到日后的使用。

3

第 3 部分
病毒和恶意软件

能够威胁到计算机安全的除了操作系统本身的不安全设置以及网络攻击外，病毒以及恶意软件也是主要的一种途径。计算机病毒的历史其实已经很久远了，再加上历史上曾经有几种广为传播，并且给很多人带来麻烦的病毒，例如 CIH、尼姆达、冲击波等，因此，现在很多人都已经对反病毒软件有所重视，习惯于给系统中安装反病毒软件，并经常更新病毒定义。然而，仅仅这样做还是不够的。

现在网上有一种口碑不是很好的程序，这类程序虽然不像病毒那样具有破坏性，但它的传播往往具有隐蔽性，同时会进行一些不友好的操作，例如给系统中弹出广告，或者统计计算机使用信息，并定期将信息发送出去。尤其是，这类软件安装到系统中后往往很不好卸载，甚至为了防止被卸载，这些软件还会使用一些病毒常用的手段，例如安装驱动、插入代码等。因为这类软件除了没有攻击性外，几乎具有病毒的其他所有的特性，因此，通常被叫做恶意软件（或者叫灰色软件、间谍软件，或流氓软件）。

因为病毒和恶意软件在很大程度上来说都是通过互联网传播的，因此，这里首先要了解如何让网络浏览器将这些危险拒之门外。

本部分，我们还会介绍怎样合理地处置包含病毒的电子邮件，如何安装自己信任并且可信的软件，以及使用 IM 软件聊天时需要注意的问题。

CHAPTER

9

第9章　安全上网

人们上网的时候一般都在做什么？浏览网页、收发电子邮件、下载和安装软件、聊天。可是，你知道这些在一般人看来很简单的操作中隐藏了多少危险吗？

在访问了一个网站之后，为什么 Internet Explorer 设置被修改并被锁定了？例如 Internet Explorer 首页被设置在一个我们不熟悉的地址，同时自己还无法修改。

笔者收到一封来自朋友的邮件，说要给我们看他的照片，双击附件的“.jpg”文件后，照片没有打开，反而有一个命令提示符窗口一闪而过，然后硬盘开始狂转，系统反应变慢。

想从网上下载一个用于播放电影的共享软件，可是安装好之后，为什么 Internet Explorer 中增加了好几个不认识的工具栏，而且系统一启动就开始弹出广告窗口？

好友有急事在网上聊天时向我们借钱，希望我们把若干数目的钱汇往一个账户。照办后，隔天见到这个朋友问起这事，他却苦着脸告诉我们，自己的密码被盗，已经有很多朋友受骗了。

这些事虽然看起来好笑，不过在互联网上每天都在发生，尤其是对于新手或者没有安全意识的人来说，自己中招了还完全没有意识到。本章介绍的就是对这些问题的防范方法。相信通过阅读本章，大家都能养成更好的安全意识。

需要注意的是，本章涉及的很多操作有大量软件都可以实现，同时这些软件的新版本几乎都提供有类似的安全选项。限于篇幅，本书不可能逐一介绍每个软件的类似设置，只介绍其中使用最广泛的或者最具有代表性的内容。如果大家也使用了本章介绍的这些软件，直接照做就可以了。如果使用的是具有同样功能的其他软件，请仔细查看这些软件提供的选项，找到类似的功能来设置。

9.1　安全浏览网页

在 Windows 平台上使用最广泛的网页浏览器就是微软的 Internet Explorer，以及使用了 Internet Explorer 浏览器内核的外壳浏览器（例如 Maxthon、Green Browser、The World 等）。因为用户数量众多，再加上对褒贬不一的 ActiveX 技术的支持，使得 Internet Explorer 浏览器看起来似乎是最不安全的浏览器。另外，由于 Internet Explorer 浏览器和 Windows 操作系

统紧密集成，甚至操作系统的某些重要功能都要借助 Internet Explorer 的某些组件来实现。因此，一旦 Internet Explorer 浏览器发现了漏洞，其影响可能是相当广泛的。

其实，Internet Explorer 在安全方面面临的问题和 Windows 几乎完全一样，Internet Explorer 显得不安全，主要还是因为用户数量众多，因此，很多病毒和恶意软件的作者都会专门研究通过 Internet Explorer 入侵系统的方法。Internet Explorer 的很多特性确实可以极大程度地增加计算机的安全，但毕竟安全和易用性是相悖的，在提高安全性的同时，易用性会被降低。因此，很多人宁愿要易用性，至于安全问题，则不那么重视，而一旦 Internet Explorer 因为不够安全的设置被攻击，这些人往往会忘记正是因为自己的错误设置才导致了安全问题，而是直接将问题归结 Internet Explorer。因此，我们必须在安全性和易用性之间做出取舍，不仅针对 Internet Explorer，针对其他任何软件的时候都需要面对这个问题。

> **提示**　需要卸载 Internet Explorer 吗?
>
> 也许有人确实不喜欢 Internet Explorer 浏览器，甚至计算机中已经安装了其他独立内核的浏览器，例如 Mozilla Firefox 或者 Google Chrome，既然 Internet Explorer 有如此多的安全问题，而又不打算使用，那么肯定有人在考虑是否可以将 Internet Explorer 彻底卸载掉。对于 Windows Vista/7 系统，这种想法完全是不可行的。上文已经说过，对于目前新版本的 Internet Explorer，已经和 Windows 紧密集成，甚至 Windows 的很多必要功能都是需要借助 Internet Explorer 的组件实现的。因此，我们可能没有直接使用 Internet Explorer，但很多操作实际上都是需要借助 Internet Explorer 才能完成。只要使用 Windows 操作系统，就不可避免地需要面对 Internet Explorer。

Windows 7 内建了 Internet Explorer 8 浏览器，本章将以该版本为例进行讨论。

需要注意的一点是，和 Windows 一样，微软也会经常给 Internet Explorer 发布补丁程序，Internet Explorer 的补丁程序可以通过 Microsoft Update 网站安装。关于 Microsoft Update 网站，以及对 Windows 进行更新的详细信息，请参考本书第 4 章补丁和更新。在继续阅读本章之前，请确保已经安装了最新的 Internet Explorer，并且安装了所有可用的补丁。

9.1.1　Internet Explorer 的一般性设置

关于 Internet Explorer 的使用方法，很多书籍或者文章都进行过介绍，因此，本书不准备过多涉及，只准备介绍 Internet Explorer 的使用过程中最常见的安全问题。这要求我们对 Internet Explorer 比较熟悉，并且了解一些基本操作。

9.1.1.1　常规和安全选项

在 Internet Explorer 主窗口的工具栏上单击“工具”按钮，从弹出菜单中选择“Internet 选项”，随后可以打开“Internet 选项”对话框。针对 Internet Explorer 的绝大部分安全设置

都是在这里进行的。下面分别针对每个选项卡中提供的选项进行介绍。

1. 常规

在“常规”选项卡下主要有两个选项需要设置，都是和隐私有关的，同时，这两个选项都位于“浏览历史记录”类别下。

在“浏览历史记录”类别下单击“删除”按钮后，可以打开图 9-1 所示的“删除浏览的历史记录”对话框，在这里可以对 Internet Explorer 保存的浏览历史进行管理。同时，如果需要经常进行这个操作，也不用那么麻烦每次都打开“Internet 选项”对话框，直接在 Internet Explorer 的“工具”菜单下单击“删除浏览的历史记录”命令即可。

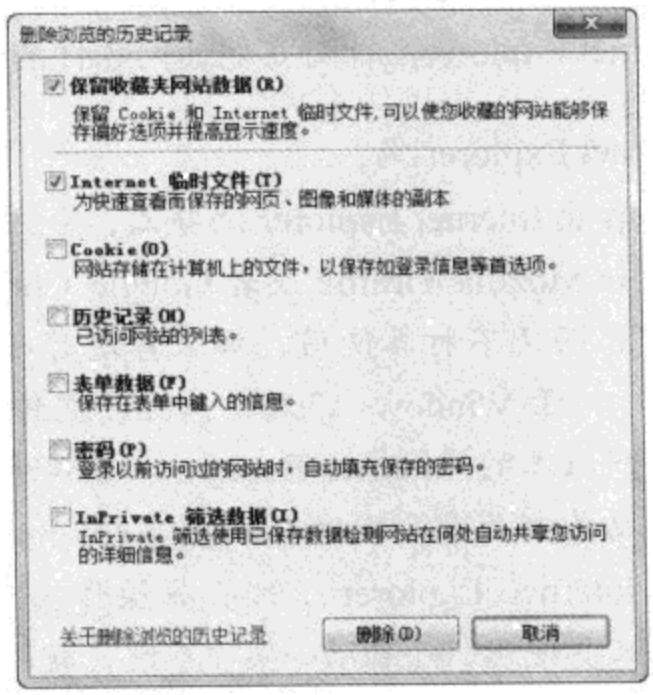


图 9-1　在这里可删除 IE 的浏览记录

在该对话框中一共可以删除 6 类不同的数据，分别单击对应的“删除”按钮即可删除。如果希望一次删除所有类型的数据，可以直接单击“全部删除”按钮。这 6 个类型的数据作用分别如下：

- **Internet 临时文件**　这个功能还是拨号上网时代的产物。当时互联网的访问速度普遍不快，为了加快网页的显示速度，几乎所有的浏览器都提供了临时文件功能。简单来说，这个功能会将我们访问的网页上的不同元素（例如，声音、图片、视频、脚本等）保存到本地硬盘上，这样刷新网页或者其他网页使用了同样的文件时就不用从互联网上将其下载到本机，而是直接使用本机保存的临时文件中的相应文件就能把网页显示出来。可以说，Internet 临时文件的使用确实可以提高网页的打开速度。在宽带上网已经普及的今天，这个功能已经不再那么重要了，甚至很多情况下，一个文件直接从网络上下载要比从硬盘上的临时文件中读取还快。这个功能主要会造成隐私上的一些问题，例如别人通过查看临时文件就会知道我们访问过哪些网站，而一旦某些网站中嵌入了病毒或者恶意软件，这些内容也会被保存到 Internet 缓存中。因此，比较明智的做法是定期清空这些文件，或者对临时文件的使用进行设置，

其设置方法请参考下文。

- **Cookie**　这是一类特殊的文件，主要用于追踪用户在访问一些网站时的信息。例如，当我们访问某个网站的时候，可能会看到网页上显示“这是您第 1 次访问本站”或者“这是您第 3 次访问本站”之类的字样，其实这就是 Cookie 的功劳。当访问大部分网站的时候，网站的服务器都会在硬盘上一个特定的位置放置一个文本文件，其中记录了访客的一些信息（例如访问次数、登录网站所用的用户名，以及加密后的密码等），正因为这样，网站才能提供一些个性化服务。举例来说，假如需要经常访问某个论坛，那么在这个论坛的登录页面上可能会提供“记住密码”之类的选项，只要选中这个选项，用户名和密码就会记录在网站的 Cookie 中，下次打开这个论坛的时候就能直接登录，而不需要再次输入自己的用户名和密码。

  Cookie 是一个很好的功能，但如果滥用也可能导致一些隐私问题或者安全问题。例如，某些网站的安全意识可能不够强，将访客输入的密码明文保存在 Cookie 中，而正常情况下，Cookie 中保存的信息应该是使用不可逆的加密算法加密过的。一旦保存明文，任何人都将可能知道我们的登录信息。

- **历史记录**　如果曾经访问过一个网站，例如，假设曾经访问过“www.microsoft.com”，当下一次打算访问这个网站的时候，在地址栏中输入地址时，可能还没有输入完整，Internet Explorer 已经很体贴地将所有建议的结果都列举出来了（如图 9-2 所示），我们只需要选择需要的地址即可直接访问。这就是历史记录的功劳，Internet Explorer 会记忆最近访问过的所有的地址，而在地址栏输入新的地址时，输入的内容就会被 Internet Explorer 用于和记住的访问历史进行比较，一旦找到了匹配的内容，就会显示出来供选择。不仅如此，在访问一些网页的时候有人可能发现了，对于打开过的链接，Internet Explorer 会使用一种不同的颜色显示，以便和没有打开过的链接区分开来。这也是历史记录的功劳。注意，历史记录功能很容易泄露我们的隐私。

图 9-2　IE 的历史记录可以帮助我们快速打开曾经访问过的地址

- **表单数据**　很多网页上都有一些文本框供我们输入信息，例如，在搜索引擎页面上输入用于搜索的关键字；或者在论坛上输入要发布的帖子内容等。经过一段时间的使用，有人可能会发现一个问题，和上面提到的历史记录功能类似，为什么在一些

文本框中输入文字的时候，Internet Explorer 会提示一些曾经输入过的内容（如图 9-3 所示）。其实这些文本框在网页上也被叫做“表单”，主要用于提交用户输入的数据。同样，Internet Explorer 会对我们在表单中输入的信息进行记录，日后一旦发现输入的信息符合保存的记录，就会将所有符合的内容显示出来，方便直接选择。和历史记录功能类似，这个功能的本意也是为了方便使用，但容易导致隐私问题。

- **密码** 这个问题就更严重了，因为一旦没能处理好，别人使用我们的用户名和密码登录，不仅会导致隐私泄露（例如，查看了我们的电子邮件），还可能存在安全问题（例如，以我们的身份在网上做坏事）。

需要注意的是，这里所说的“密码”，仅仅指在 Internet Explorer 中登录网站时输入的密码，而不是 Windows 账户密码或者其他密码。当访问一个需要登录的网站，并在相应的文本框（也是表单，但和一般的表单有所不同）中输入自己的用户名和密码，开始登录的时候，Internet Explorer 会用一个对话框提示我们是否保存密码（如图 9-4 所示）。在这个对话框上有三个选择，如果希望保存，可以单击“是”；如果不希望保存，可以单击“否”。如果不希望保存，同时也不希望以后保存任何网页的登录密码，可以选中“不再保存密码”。

图 9-3 IE 可以帮我们保存在网页上输入的信息

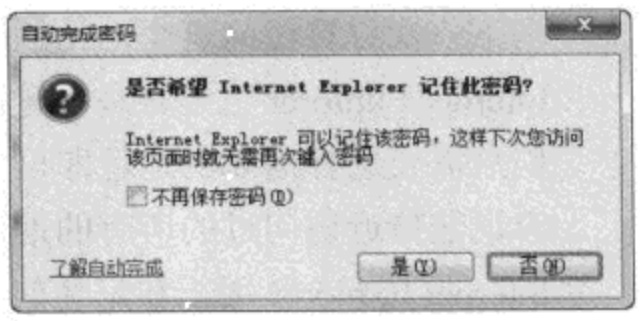


图 9-4 IE 会询问是否保存密码

在选择了保存密码的选项后，下次登录同一个网页时，直接在用于输入用户名和密码的文本框中双击，Internet Explorer 就会显示出保存的用户名和密码（如图 9-5 所示），供我们快速登录。

图 9-5 通过保存的登录信息实现快速登录

如果在一个网页上有多个账户登录过，并且都保存了登录密码，那么这里就会列出保存的所有条目，选择后即可使用相应的账户登录。

- **InPrivate 筛选数据**　InPrivate 筛选是 Internet Explorer 8 中的新功能，该功能可以对日常的网页访问情况进行统计，并将网页中包含的信息进行分析。如果认为来自某个站点的信息同时出现在多个其他站点中，那么就可以将这个站点的内容直接过滤掉。有关该功能的用途和使用方法，会在下文详细介绍。而通过这里的选项可以将 InPrivate 功能统计的信息全部删除。

需要注意的是，对于 Windows 7 这类多用户操作系统，如果每个使用计算机的人都有各自独立的账户，并且每个人的账户都有密码保护，那么上述问题将不再是问题。毕竟这些隐私信息都是保存在每个人的配置文件中的，除了管理员，一般用户都无法直接访问别人的配置文件。因此，在多用户操作系统中，给每个人准备一个账户，不仅可以提高系统安全，而且可以极大地给我们带来便利。

如果需要多人共用一个账户，那么每次使用完之后都删除记录显得有些麻烦，这时候可以让 Internet Explorer 代替我们进行。我们只要在 Internet 选项对话框的“常规”选项卡下选中“退出时删除浏览历史纪录”，这样每次关闭最后一个 Internet Explorer 窗口的时候，程序就会自动将所有的浏览记录都删除。如果对这个功能还是不放心，还可以试试看 Internet Explorer 8 中新增的 InPrivate 浏览，这个功能会在下文中详细介绍。

另外还有一点，有时候我们可能只希望删除记忆的某一条记录，而不是全部删除。例如，希望删除某个网站上的某个账户的登录密码，而保留记住的其他密码，或者希望删除某个表单数据，同时保留其他表单数据。这时候该怎么办？

以表单数据为例，在图 9-3 中，假设希望删除其中的“windows vista”这个条目，只需要输入“w”，让 Internet Explorer 将所有的条目都显示出来，然后将鼠标指针放在想要删除的条目上，按下键盘上的“Delete”键即可。

在 Internet 选项对话框的“常规”选项卡下单击“浏览历史记录”下的“设置”按钮，可以看到图 9-6 所示的“Internet 临时文件和历史记录设置”对话框。

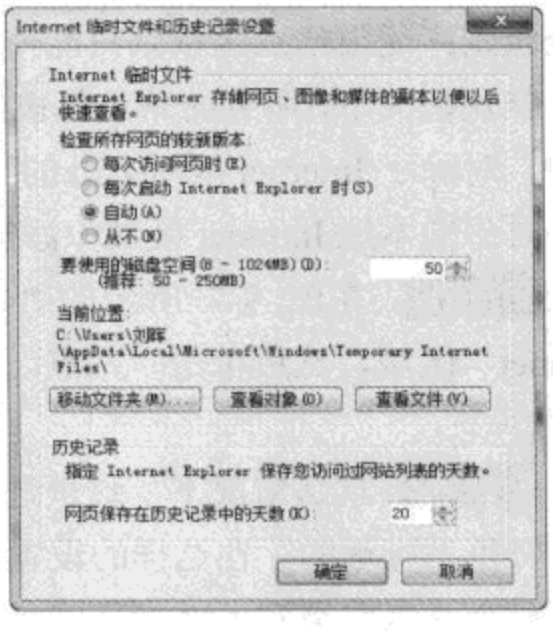


图 9-6　对 IE 的临时文件使用情况进行设置

上文已经说过，对于目前的宽带网络来说，Internet 临时文件对网页打开速度的影响已经很小了，因此，完全可以在这里将其设置在一个比较小的值，或者调整临时文件的默认保存位置。

首先，如果要调整临时文件使用的硬盘空间数量，可以在“要使用的磁盘空间”文本框中以 MB 为单位进行设定。这里不建议设置得太小，因为虽然有宽带网络可以帮助我们下载快速组成网页的文件，但有时候可能会频繁刷新某些页面，例如论坛，在这种情况下，一个较小的临时文件设置（例如 50～100MB 之间）是比较合理的，而尽量不要像以前拨号上网那样设置

上百兆字节的临时文件。

如果希望更改临时文件的默认保存位置，可以单击“移动文件夹”按钮，并在随后出现的“浏览文件夹”对话框中指定新的保存位置。如果系统盘空间比较紧张，但又需要使用大量的临时文件，或者不希望频繁写入临时文件导致硬盘空间的碎片，那么可以用这种方法移动临时文件的位置。

最后，还可以在“网页保存在历史记录中的天数”选项下指定 Internet Explorer 保存多少天的网页浏览记录。如果账户只是自己一个人用，并且希望能够通过历史记录了解自己浏览过的页面内容，建议在这里设置一个比较长的天数。

2. 安全

“Internet 选项”对话框的安全选项卡如图 9-7 所示，和 Internet Explorer 有关的安全选项大部分都需要在这里设置，因此，这也是本节的重点。

首先需要了解安全区域的含义和作用。互联网上有很多站点，根据作用和我们的信任程度，这些站点可以被分为不同的类别。例如，对于陌生的第一次访问的站点，需要采取一种安全设置；对于企业内部的局域网站点，可被信任，可以采取另一种安全设置；对于某些关键的站点，例如网上银行，不仅要信任，而且还要确保一定的安全；对于不被信任，同时有一定危险性，但又必须访问的站点，则又需要采取一种安全设置。

为了能够让我们用一种更加方便的办法对不同站点设置不同的安全级别，Internet Explorer 中提供了安全区域的概念。现在的 Internet Explorer 有“Internet”、“本地 Intranet”、“可信站点”和“受限站点”4 个安全区域，对于这 4 个安全区域，可以使用默认的“低”、“中低”、“中”、“中高”，以及“高”5 个不同的安全级别，越是高级的安全级别，对安全的要求就越严格，同时限制也越多。另外，Internet Explorer 对两个特殊的安全区域还有更加严格的安全设置，例如，Internet 区域的站点就只能选择“中”、“中高”和“高”这三个安全级别；受限站点区域则只能使用“高”这个安全级别。

默认情况下，所有的站点都被归类于 Internet 区域，除非该站点的地址被添加到其他区域中。对除了 Internet 区域之外的三个区域，具体的操作有所不同，下文将分别介绍。

要想向本地 Intranet 区域中添加站点，请这样操作：

STEP 01 在图 9-7 所示的“Internet 选项”对话框的安全选项卡下单击选中“本地 Intranet”区域，然后单击“站点”按钮，随后将打开图 9-8 所示的“本地 Intranet”区域对话框。

STEP 02 默认情况下，这里选中的是“自动检测 Intranet 网络”选项，同时其他选项都是灰色不可选的。在这样的设置下，Internet Explore 会根据访问的站点地址自动判断是否将一个站点归类到本地 Intranet 区域，一般情况下也建议使用该设置。如果希望自己决定将符合哪些条件的站点当做是本地 Intranet 站点，可以反选“自动检测 Intranet 网络”选项，然后选择下列设置：

图 9-7　IE 的“安全”选项

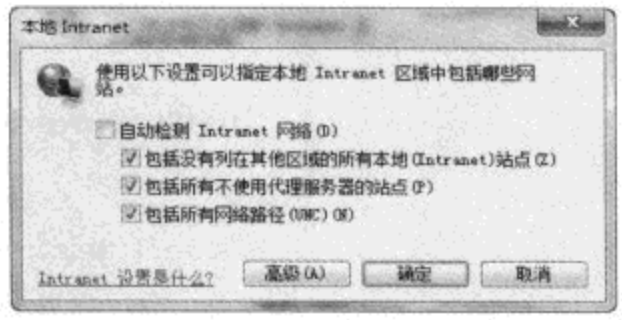


图 9-8　在这里设置本地 Intranet 选项

- **包括没有列在其他区域的所有本地（Intranet）站点**　选中该选项后，任何一个位于本地局域网中的站点，只要没有被添加到其他区域，都将被认为是本地 Intranet 站点。
- **包括所有不使用代理服务器的站点**　选中该选项后，任何站点只要可以不用通过代理服务器访问，都当做是本地 Intranet 站点。该选项主要适合设置了代理服务器的企业网络，同时选择该选项的时候需要注意，例如，假设有一个互联网上的站点，网络管理员设置了访问该互联网站点的时候不需要通过代理服务器，那么 Internet Explorer 也会对这个互联网站点应用本地 Intranet 站点的安全设置。
- **包括所有网络路径（UNC）**　选中该选项后，任何使用 UNC（Universal Naming Convention，通用命名约定）路径（例如 http://webserver）访问的站点都会被看做是本地 Intranet 站点。

STEP 03　如果希望更进一步设定本地 Intranet 站点，例如，只希望某些明确指定的站点才被应用本地 Intranet 区域设置，而其他没有明确指定的，哪怕位于本地网络中的站点都被应用 Internet 区域设置，则可以在反选“自动检测 Intranet 网络”选项后不要选择其他三个选项，接着单击“高级”按钮，随后可以看到图 9-9 所示的“本地 Intranet”对话框。

STEP 04　在“将该网站添加到区域”文本框中输入要添加的站点的地址，然后单击“添加”按钮即可。如果希望删除一个已经添加的站点，则可以在选中该站点后单击“删除”按钮。经过上述设置，只有在这里添加过的站点才会被应用本地 Intranet 区域的安全设置，而其他站点，哪怕位于本地局域网中，也会被应用 Internet 区域的安全设置。

要想向可信站点区域添加站点，请这样操作：

STEP 01　在图 9-7 所示的“Internet 选项”对话框的“安全”选项卡下单击选中“可信站点”区域，然后单击“站点”按钮，随后将打开类似图 9-9 所示的“可信站点”对话框。

图 9-9　指定需要应用本地 Intranet 设置的站点

STEP 02 在“将该网站添加到区域”对话框中输入要添加的网站地址，然后单击“添加”按钮。如果希望删除一个已经添加的地址，请从列表中单击选中目标地址，然后单击“删除”按钮。

STEP 03 默认情况下，只有使用加密连接的网站（网站地址使用“https://”开头）才被允许添加到可信站点区域，如果希望添加没有加密的网站，请取消对“对该区域中的所有站点要求服务器验证（https:）”选项的选择。

要想向受限站点区域添加站点，也只需要在图 9-7 所示的“Internet 选项”对话框的安全选项卡下单击“受限站点”区域，然后按照添加可信站点那样添加即可。

窍门　站点地址的选择

在向上述任何一个区域添加站点的时候，都可以通过合理地输入站点以避免不少工作。例如，假设有个网站的完整地址是“http://www.site.com”（这是一个虚构的地址），我们将其添加到可信站点区域，但同时该域名下还有其他站点，例如“http://subsite.site.com”，也希望将该站点添加到可信站点区域。这时候只要向可信站点区域添加一个“site.com”就可以了，这样，所有该域名及其子域名下的站点都会被 Internet Explorer 看做是可信站点。当然也可以使用通配符，例如，将“app.*.site.com”添加到可信区域后，“app.subsite1.site.com”就会被应用可信站点区域的安全设置，但“app1.subsite2.site.com”就不会被应用。

如果希望查看一个区域的安全级别，或者选择使用不同的安全级别，请首先单击选中该区域，然后拖动下方的滑块调整安全级别。如果单击“自定义级别”按钮，在随后出现的对话框中还可以针对当前选中的区域详细调整不同的安全设置。如果在详细调整了安全设置后希望将设置恢复为默认级别，可以单击“将所有区域重置为默认级别”按钮。

窍门　理性对待 Internet 区域的安全级别设置

在 Internet Explorer 的默认设置中，只能对 Internet 区域使用三个比较高的安全级别，这主要是为了防止用户无意中选择了较低的安全级别，而给 Internet Explorer 甚至整个系统带来安全隐患。然而，有时候又必须使用比较低的安全级别，例如国内的某家 ISP，需要给 Internet Explorer 安装一个插件，以便实现拨号和身份验证操作。正常情况下，Internet Explorer 不允许从 Internet 区域的站点中安装不包含数字签名的插件，然而该公司提供的插件并不包含数字签名。为了成功安装，必须自定义 Internet 区域的安全级别，允许安装未经签名的插件，实际上，该 ISP 公司在给客户安装网络的时候也就是这样做的。然而遗憾的是，在检查过该公司员工设置过的很多计算机后，我们发现一个问题，该公司的员工在降低了 Internet 区域的设置，成功安装了自己的插件后，并没有将设置还原，这将直接导致日后用户可能会把任何不包含数字签名的恶意插件安装到系统中来。当然，这也许只说明该公司的某些员工安全意识不够强，不具有代表性，但这也从侧面说明了安全并不是某一家公司就能做好的，这往往需要很多人的通力配合。

如果因为各种原因需要对某个安全区域使用自定义的安全级别，请单击选中该区域，然后单击“自定义级别”按钮，随后可以打开图 9-10 所示的“安全设置”对话框。对于上文提到的 4 个不同的安全级别，这里的选项都是相同的，不同的只是每个选项的具体设置。下文会通过 Internet 区域详细介绍每个选项的含义以及建议设置。

图 9-10　在这里可以自定义安全区域的详细设置

在修改下列设置的时候，大部分设置都有三个不同的选项，其含义如下：

- **禁用**　禁止使用选项描述的功能。
- **启用**　允许直接使用选项描述的功能。

- **提示** 在需要使用选项描述的功能时提示用户，并提供允许和禁止使用的选项供用户选择。

下文中对于每个选项提供的默认值，如非特别说明，都是指针对 Internet 区域的。而同一个选项针对不同区域以及不同的安全级别，其设置有可能不同。

（1）.NET Framework/XAML 浏览器应用程序。

XAML 是 Extensible Application Markup Language（可扩展应用程序标记语言）的缩写，该选项决定了是否允许在浏览器中使用 XAML 应用程序，默认情况下，除了受限站点外，其他安全的区域都是被启用的。建议不要随便更改该选项的设置。

（2）.NET Framework/XPS 文档。

XPS（XML Paper Specification）是微软新发布的一种文档格式，该格式类似 Adobe 的 PDF 格式，可以跨平台在不同设备上显示完全一致的文档内容（详细信息请访问 http://tinyurl.com/yzalt5j）。默认情况下，我们可以使用安装了加载项的 Internet Explorer 查看 XPS 文档，但前提是启用该选项。默认情况下，除了受限站点外，其他安全区域都是被启用的。由于 Windows 7 已经内建了 XPS 查看器，如果不希望使用 Internet Explorer 查看 XPS 文档，请禁用该选项。

（3）.NET Framework/松散 XAML。

松散 XAML 是.NET Framework 的一项新功能，可以让我们不经过编译就直接在浏览器中运行来自本地硬盘或者互联网上的 XAML 文件。默认情况下，除了受限站点外，其他安全区域都是被启用的，如果不希望 Internet Explorer 使用该功能，则可以将其禁用。

（4）.NET Framework 相关组件/带有清单的权限组件。

该选项决定了对于包含权限清单的网页组件是否允许按照清单中所声明的权限来执行组件。权限清单是一种特殊的文件，用于声明执行相关代码时所需的权限。这一点与本书第 4 章介绍 UAC 时提到的应用程序清单文件非常类似。

通常情况下，如果不是访问特定网站时遇到问题，建议不要修改该设置，以免影响整体的安全性。

（5）.NET Framework 相关组件/运行未用 Authenticode 签名的组件，.NET Framework 相关组件/运行已用 Authenticode 签名的组件。

Authenticode 是一种数字签名机制，该功能主要为了对代码、脚本和 ActiveX 控件提供签名验证机制，而带有 Authenticode 签名的组件可以帮助我们了解组件的来源是否可信。

> **注意** 组件的数字签名只能证明该组件的来源，并不能证明其对 Windows 绝对无害。例如，网上口碑很差的某些 Internet Explorer 插件，虽然带有数字签名，但很多人并不喜欢，依然将其称做“流氓软件”。

因此，对于“运行未用 Authenticode 签名的组件”这个设置，建议选择“禁用”或者“提

示”；对于“运行已用 Authenticode 签名的组件”这个设置，建议选择“启用”或者“提示”。

（6）ActiveX 控件和插件/ActiveX 控件自动提示

如果访问的网页需要安装 ActiveX 控件，那么取决于该选项的设置，Internet Explorer 的行为会有所不同。如果禁用该选项（默认设置），那么当需要安装 ActiveX 控件的时候，Internet Explorer 会在地址栏下方显示图 9-11 所示的黄色信息栏（关于信息栏的详细信息请参考本书 9.1.1.2 节“信息栏”），提醒我们当前网页需要安装 ActiveX 控件，在单击信息栏，并选择安装后，还需要通过 UAC 的提升（如图 9-12 所示）。

图 9-11　用信息栏通知有控件需要安装

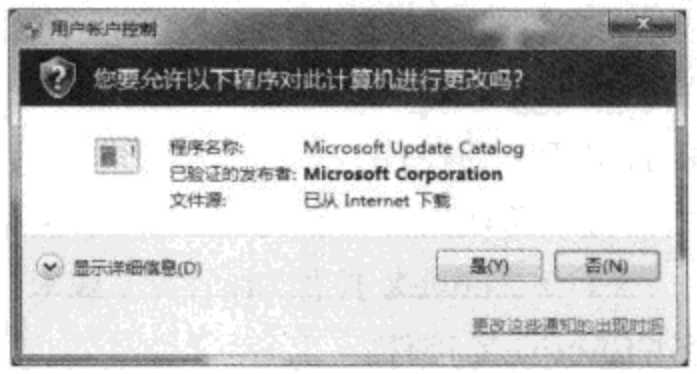


图 9-12　随后还需要通过 UAC 提升权限

如果启用该选项，那么在需要安装 ActiveX 控件的时候，Internet Explorer 将不再显示信息栏，只需要进行 UAC 的提升，然后就会自动安装。

对于这个选项，建议使用默认的“禁用”设置，这样在需要安装 ActiveX 控件的时候，Internet Explorer 需要进行两次提示，尤其是对于使用 UAC 的 Windows 7，第二次提示还需要经过用户账户控制功能的提升，这就进一步限制了只有管理员用户才可以安装 ActiveX 控件。这样虽然麻烦了一些，不过可以尽量避免一般用户随便安装控件，导致系统出现各种问题。而且第一次的提示是通过信息栏的方式进行的，大部分普通用户在浏览网页的时候，往往会忽略这一不起眼的提示，因此，可进一步降低被安装恶意控件的可能性。

（7）ActiveX 控件和插件/对标记为可安全执行脚本的 ActiveX 控件执行脚本。

为了实现一些特殊的功能，很多 ActiveX 控件必须要能够作为脚本执行，然而这种操作可能会带来安全隐患。为了避免这些问题，提供控件的开发商可以给控件添加两种标记：“可安全初始化的”和“可安全执行脚本的”。该选项决定了对于标记为“可安全执行脚本的”控件和插件是否允许执行脚本。对于该选项，建议保持默认的“启用”设置，以免影响控件的正常使用。当然，如果信不过提供控件的开发商，也可以设置为“提示”，这样，每当控件需要执行脚本时，Internet Explorer 就会发出询问，允许我们允许或者拒绝，也可以直接选择“禁用”，将其禁用。

（8）ActiveX 控件和插件/对未标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本。

和上一条选项的用途类似，该选项可以决定对于未标记为安全的脚本是否允许其运行或者初始化。同样，建议的设置也请参考上一条选项。

（9）ActiveX 控件和插件/二进制和脚本行为。

二进制行为使得二进制程序可以链接到或者控制 HTML 内容，而该选项决定了是否允许网页上包含的元素使用二进制行为和脚本行为，同时这些内容是被默认启用的。因为这些功能可以对系统进行的操作太多，因此，建议将其禁用，或者至少设置为“提示”。

（10）ActiveX 控件和插件/仅允许经过批准的域在未经提示的情况下使用 ActiveX。

该设置主要适用于企业环境，例如，企业中通常会使用 B/S（浏览器/服务器）架构的 OA 或 CRM 系统，而为了实现某些特殊的功能，这些系统可能会需要给浏览器安装某些 ActiveX 控件。为了便于此类 B/S 系统的使用，管理员可以通过设置，让企业中所有计算机的浏览器在访问内部站点（或其他经过批准的域）时，可以忽略 ActiveX 的相关警报，直接启用所需的控件。

对于普通用户，该选项的作用不大，因此，可以保留默认设置，不要随意修改。

（11）ActiveX 控件和插件/下载未签名的 ActiveX 控件，ActiveX 控件和插件/下载已签名的 ActiveX 控件。

网页上提供的 ActiveX 控件可能是带有数字签名的，也可能是不带的。数字签名可以保证一个控件在发布后没有经过篡改（因为更改控件文件的内容会导致签名失效），同时也可以告诉我们控件是由谁开发的。例如，图 9-12 中列举的控件就是由 Microsoft Corporation 发布的。

因为对控件添加数字签名需要不少费用和进行很多额外的工作，因此，很多安全意识薄弱的软件开发商提供的控件并不包含数字签名（例如上文提到的国内某个 ISP 的拨号和身份验证控件，而顺利安装这种控件的方法就是临时将“下载未签名的 ActiveX 控件”选项设置为“启用”）。这两个选项决定了对于带有或者不带数字签名的控件是否允许下载。建议对不带签名的控件选择“提示”或“禁止”；对带有数字签名的选择“允许”。

这里再次提醒注意，带有数字签名并不能表示其对系统就是无害的，只要花钱购买商业数字证书，任何人都可以开发出带有数字签名且被 Internet Explorer 认可的插件。

（12）ActiveX 控件和插件/允许 Scriptlet。

Scriptlet 是 DHTML（一种网页编写语言）中使用的脚本。既然是脚本，那么在执行的时候就可能有危险，因为这种脚本的使用不是很普遍，因此，默认情况下，该选项是被禁用的，除非特别需要，否则不建议启用它。

（13）ActiveX 控件和插件/允许运行以前未使用的 ActiveX 控件而不提示。

该选项决定了对于已经安装到系统中但是还没有使用过的插件，在第一次使用的时候是否对用户进行提示，其默认值是“禁用”。这里建议将其设置为启用，这样当一个控件第一次运行的时候，我们至少会知道有一个新的控件要首次运行了，而一旦运行后，系统出现了任何问题，我们可以先从这个首次运行的控件上找原因。

通常来说，Internet Explorer 的大部分控件都是在访问某些网页的时候安装的。然而有些软件为了实现某些功能，往往也需要给 Internet Explorer 安装控件，并且在安装软件的时

候会自动进行。因此，这类控件会在我们不知情的前提下安装到 Internet Explorer 中。为了提醒我们注意，当这样的控件首次运行的时候，默认情况下，Internet Explorer 会禁止该控件的运行，并显示信息栏，询问我们是否允许运行。

如果将该选项设置为启用，对于一个控件，在运行一次后，再次运行将不会提示。

（14）ActiveX 控件和插件/运行 ActiveX 控件和插件。

该选项决定了网页是否运行控件和插件。和其他设置相比，该设置增加了一个名为“管理员认可”的选项，在选择该选项后，只有管理员批准过的控件和插件才可以运行，不过这个选项通常用于大型企业网络中。对于一般用户，建议将其选择为“启用”，这样才不会影响到网页的正常显示，要知道，现在网页中的很多内容都是通过控件和插件产生的，例如 Flash、嵌入的视频或音频文件等。

如果真的很担心运行控件后带来的安全问题，也可以将其禁用。但这种情况下建议对可信站点区域启用，并将确实需要运行控件和插件的站点添加到可信站点中。这样在保证安全性的同时，还可以正常查看关键的网页。

（15）ActiveX 控件和插件/在没有使用外部媒体播放机的网页上显示视频和动画。

这个选项决定了是否允许一些不受信任的媒体播放软件播放嵌入到网页上的媒体文件。我们常见的媒体文件格式，以及播放器软件基本上都是受信任的。因此，对于该选项，可以使用默认值“禁用”。

（16）脚本/Java 小程序脚本。

该选项决定了是否允许 Internet Explorer 执行网页上的 JavaScript 脚本。注意，这里所说的“Java 小程序脚本”和 Sun 公司的“Java”语言是两回事。虽然很多恶意网页使用 JavaScript 脚本干坏事（例如，锁定 Internet Explorer 首页设置或者修改系统注册表），不过更多的网页在使用 JavaScript 实现一些必要的功能（例如，定时刷新页面或者弹出对话框）。因此，不建议将该选项设置为禁用。

如果确实很担心恶意网页上的 JavaScript 脚本对系统有影响，可以对反病毒软件进行恰当的设置，因为现在主流的反病毒软件几乎都包含了对网页内容的监控，如果遇到网页上包含了恶意脚本，都会进行拦截。有关反病毒软件的使用，请参考本书第 10 章。

（17）脚本/活动脚本。

除了上文提到的 JavaScript 脚本，网页中常见的脚本还包括 VBScript，要执行这些脚本，系统中必须安装了对应的执行引擎。而该选项决定了是否允许网页调用引擎执行这些脚本。对于该选项，建议保持默认设置，并将安全问题交给反病毒软件解决。

（18）脚本/启用 XSS 筛选器。

XSS（Cross-site scripting，跨站点脚本）是近些年比较常见的网络攻击方式，有关该攻击方式的详细信息，可参考 http://tinyurl.com/yakd5uc。为了防范这种攻击，Internet Explorer 8 中提供了 XSS 筛选器功能，该功能可对访问的网页内容进行检测，一旦检测到网页中存在注入式 XSS 代码，Internet Explorer 8 就可以禁止此类代码的执行，但网页的其他部分还是可以

正常显示。

有关 XSS 筛选器工作原理的详细信息，可参考 http://tinyurl.com/6d735w。作为一般用户，该选项可保留默认设置，不建议随意修改。

（19）脚本/允许对剪贴板进行编程访问。

当我们选中一个文件，按下“Ctrl+C”组合键，或者当我们在字处理软件中选中一段文字，按下“Ctr+C”组合键后，所选的内容就会被复制到剪贴板中。剪贴板实际上是内存中的一块区域，可以保存任何类型的数据，复制到剪贴板中的数据可以粘贴到对应的程序中。如果剪贴板中复制了某个文件，那么就可以在 Windows 资源管理器中进入到不同的文件夹，并粘贴文件到新的位置；如果剪贴板中保存的是一段文字内容，则可以将其粘贴到其他支持文字输入的位置。

其实网页也是可以对剪贴板进行访问的。这本来是一个体贴的功能，例如，很多人在网页上发帖子或者发邮件的时候可能都会遇到这样的问题：自己花了很长时间写的文字，在发送的时候，因为网络故障或者登录超时而没有发送成功，而之前写好的内容全部都消失了。那么在本选项对应的功能帮助下，一些注重细节的设计师就会在自己设计的网页上增加对用户剪贴板的读写功能，例如在写下文字发送之前，网页首先会将写出来的文字复制到用户的剪贴板中，这样一旦因为某种原因没能发送成功，至少用户的剪贴板中还保存有相关的信息。

然而，任何东西在滥用后都可能导致问题。假设有一些恶意网页，专门通过读取访客剪贴板中的内容的方法来窥探用户隐私，我们在做其他工作时保存在剪贴板中的数据（这个数据也许是重要客户的电话号码，或者自己的银行账号等）就可能会被恶意网页读取，造成泄密。

对于该选项，建议选择“提示”，并且在浏览网页的时候密切注意提示信息。如果在浏览网页的时候遇到了图 9-13 所示的对话框，那就要小心了。如果是在论坛上发帖子的时候遇到，还可以理解。但如果打开一个陌生的网站，没有在网页中输入任何文字，突然跳出了这样的提示，那么这个网站肯定是有问题的。

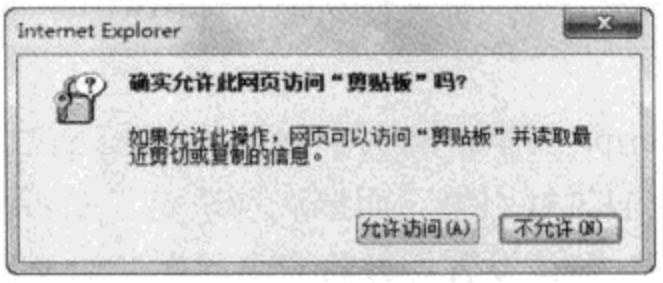


图 9-13　当网页试图访问剪贴板时，IE 会发出询问

（20）脚本/允许网站使用脚本窗口提示获得信息。

当我们注册某些网站的时候，网页上可能会以脚本的形式跳出一个窗口，提示输入一些注册信息，例如用户名或者电子邮件地址等（对于通过普通 HTML 语句编写的网页表单，

则不受此限制）。由于使用此类设计的网页越来越少，因此，为了确保安全，该功能默认是被禁用的。但如果需要，也可以将其启用。

（21）脚本/允许状态栏通过脚本更新。

如果启用这个功能，那么网页将可以使用脚本在 Internet Explorer 浏览器的状态栏显示一些信息（可能是滚动新闻，或者其他提示信息）。这个功能会带来两个问题：首先，有些网页设计得不够合理，会以很高的频率在状态栏滚动显示新闻或者其他来自网站的消息，这样很容易干扰我们的注意力，让人变得烦躁。

另外，通过该功能，网站可以伪造 Internet Explorer 的提示信息。举一个最简单的例子，当我们在网页上用鼠标指向一个链接后，在 Internet Explorer 的状态栏左侧就会显示该链接的目标网页地址。这很正常，但如果浏览的是一个手法低劣的钓鱼网页（有关网络钓鱼的详细信息，请参考 9.4 节），网页上提供了到某银行的链接，并以银行的身份告诉我们，由于系统升级，需要在所谓的“官方网站”上输入自己的账号和密码以便确认升级成功，同时利用脚本，让鼠标指向到“官方网站”的链接时在状态栏显示真正的银行网站地址，但实际上链接的目标地址是伪造的网站，这种时候如果不够小心，就容易受骗（其实很多人都习惯于通过 Internet Explorer 状态栏中显示的内容了解一个超级链接的目标地址是到哪里的）。

因此，不管是为了安全，还是不想看到状态栏上的滚动消息，都建议禁用该选项。

（22）其他/持续使用用户数据。

通过使用该功能，网站将可以在用户的硬盘上保存和当前用户或者当前会话有关的信息，这样用户在短时间内使用该网站的时候，就可以使用统一的设置（在这一点上和 Cookie 类似，但该功能不等于 Cookie）。建议对该选项使用默认的设置。

（23）其他/基于内容打开文件，而不是基于文件扩展名。

在启用该功能后，每当浏览器需要向网站请求一个文件（可能是用于下载的文件，或者用于显示网页的图片或脚本），浏览器会首先读取目标文件的前 200B，并根据其中的信息判断文件的类型，然后使用相应的方式处理目标文件。例如，对于某些动态网页，以论坛为例，在下载论坛上的一个附件时，下载地址的一部分可能是“file.aspx?id=123456”，在这种情况下，Internet Explorer 会首先下载目标链接的前 200B，然后判断要下载的文件的类型，接着才会提供各种选项，例如，直接作为网页的一部分显示出来，或者允许保存或直接打开。建议使用默认设置，启用该功能。

（24）其他/加载应用程序和不安全文件。

所谓的不安全文件，是指一些可以执行的文件，以扩展名来看，包含的文件类型有：.asp、.bas、.bat、.chm、.cmd、.com、.exe、.lnk、.inf、.reg、.isp、.pcd、.mst、.pif、.scr、.hlp、.hta、.js、.jse、.url、.vbs、.vbe、.ws 和.wsh。如果该选项设置为“启用”，那么对于这些类型的文件以及程序，将直接运行，不经询问。显然，这样不够安全，我们可以将其设置为“提示”或者“禁用。”

（25）其他/将文件上载到服务器时包含本地目录路径。

该选项决定了当时用 Internet Explorer 通过 HTTP 或者 FTP 协议上传文件到服务器的时候，是否在上传信息中包含文件的本地路径信息。建议使用默认的“启用”选项，否则可能导致在某些网站上传文件失败。

（26）其他/跨域浏览子框架。

该选项决定了是否允许在浏览某个域的网页时在网页中打开来自其他域的子框架，为了提高安全性，建议使用默认的“禁用”设置，或者设置为“提示”。

要理解这个选项的作用，必须明白什么是子框架，请看图 9-14 所示的网页。

图 9-14　带有框架的网页

注意图 9-14 中鼠标指针所在的位置，鼠标指针变成了可拖动的样子，可以左右拖动调整两侧网页的宽度。这就是一个应用了嵌入框架的典型网页，在图 9-14 中至少有三个框架（分别位于鼠标指针所在位置的左右两侧，以及这两个框架上方横跨页面的内容区域），浏览器地址栏中显示的网页地址既不是左侧框架的地址，也不是右侧框架的地址，而是主页面的地址。这种方式的网页设计主要是为了便于快速浏览大量的页面，例如，在左侧框架单击一个链接后，对应的内容就会在右侧框架中打开，而并不需要刷新整个页面。

这种网页的危险之处在于无法直观地看到每个框架对应页面的地址。例如，假设单击左侧框架中的一个链接，在右侧框架中打开了一个与主网页和左侧框架页面不在同一个服务器上的页面，这时候我们并不容易知道，我们也许以为自己还在左侧框架对应页面所在的服务器上（这个服务器也许是被我们信任的）。所以，就想当然地认为右侧框架对应的页面也在同一个服务器上（这个服务器可能并不是我们信任的）。

在禁用该选项后，一旦某个框架中需要打开一个与主网页不在一个服务器上的页面，Internet Explorer 将会拒绝。为了保证正常浏览，建议也可以设置为“提示”，这样当 Internet Explorer 试图打开其他服务器上的子框架时会对我们发出提示。

（27）其他/没有证书或只有一个证书时不提示进行客户端证书选择。

当访问一些需要高安全性的站点（例如网络交易或者网络银行）的时候，为了保证安全，这些站点往往会进行加密，同时需要提供数字证书才能访问。如果系统中只有一个用于访问某网站的数字证书，那么在启用该选项的情况下，Internet Explorer 就会直接使用唯一的证书访问该网站；如果系统中有多个可用的证书，或者禁用了该选项，Internet Explorer 就会显示一个对话框，供我们选择想要使用的证书。

对于该选项，建议设置为“禁用”，毕竟这样做之后，每当访问需要证书的网站时，Internet Explorer 都会显示“询问”对话框，我们可以将其看做是一个提醒，提示我们将要访问的是一个加密网站。

（28）其他/使用 SmartScreen 筛选器。

SmartScreen 筛选器的主要目的是为了防范仿冒网站，这属于一种社会工程学诈骗。

仿冒网站是指利用社会工程学原理进行网络欺诈的网站，这种手法有时候也叫做“网络钓鱼”。例如，招商银行的网站地址是“www.cmbchina.com”，如果有人开办了一个地址是“www.cnnbchina.com”的网站，将站点页面设计得和招商银行网页一模一样，并通过各种方法诱骗招商银行的用户在这个假冒的招行网站上输入自己的账号和密码，就可以利用这些信息行窃。

为了防范这种钓鱼攻击，Internet Explorer 8 中包含了 SmartScreen 筛选器功能。简单地说，微软维护了一个在线数据库，其中包含了很多已知的仿冒网站地址，每当我们访问一个地址的时候，Internet Explorer 都会自动将访问的地址信息提交到数据库中进行查询，如果查询到匹配的项目，证明当前网站是仿冒网站，并给我们发出提示。

（29）其他/使用弹出窗口阻止程序。

该选项决定了是否启用 Internet Explorer 的弹出窗口拦截功能，有关该功能的详细信息请参考下文。

（30）其他/特权较少的 Web 内容区域中的网站可以定位到该区域。

该选项可以防止低特权级别的内容初始化到高特权级别内容的连接。这个功能主要是为了防范恶意攻击的，因此，最好使用默认的“启用”设置。

（31）其他/提交非加密表单数据。

当我们第一次在网页上输入文字，并发送出去的时候，Internet Explorer 会提醒我们因为没有加密，任何人都能看到我们提交的内容，并询问是否继续。如果将该选项设置为“提示”，那么以后每次提交时都会询问；如果设置为“启用”，以后就不会提示；如果设置为“禁用”，将无法在不加密的网页上提交数据。

如果希望清理已经提交的数据，请参考 9.1.1.1 节中“常规”一段的介绍。

（32）其他/通过域访问数据源。

该选项决定了当我们访问位于服务器 A 上的网页时，是否允许网页从服务器 B 获取外部数据。通常情况下，正常网页如果要引用网页服务器之外其他服务器上的数据，这些服务器至少应该在同一个域中，这种情况不会受到该选项的限制。该选项只能限制网页服务器和数据来源服务器不在一个域的情况下，往往恶意网页会这样做，因此，建议该选项使用默认的“禁用”设置。

（33）其他/拖放或复制和粘贴文件。

这个选项主要是为了通过 Internet Explorer 访问 FTP 服务器准备的。在启用该功能后，我们可以将文件或文件夹从本地硬盘拖放到 Internet Explorer 窗口中，这样文件就会被上传到 FTP 服务器（只要有上传权限）；而从服务器拖动到本地则可以自动下载。因此，如果要使用 Internet Explorer 访问 FTP 内容，建议启用该选项，否则可以禁用。

（34）其他/显示混合内容。

当我们在访问一些加密网站的时候，很可能会看到图 9-15 所示的对话框。

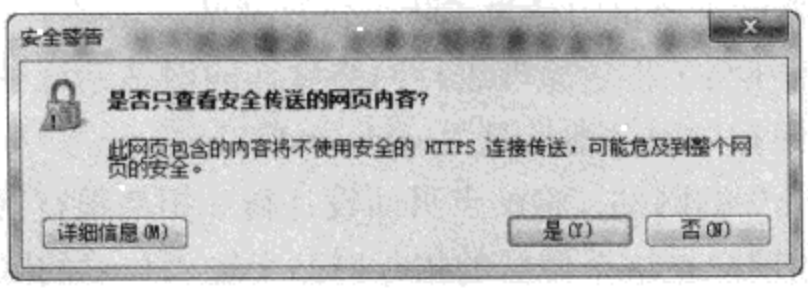


图 9-15　页面包含混合内容时 IE 的提示

这是什么意思？假设我们在访问一个加密的网站 A，网站的页面上引用了一个位于服务器 B 上面的图片，而服务器 B 是不需要加密访问的。这种加密和不加密内容同时出现在一个页面上的现象就是混合内容。

对于这个选项的设置，有不同的看法。如果比较在意安全性，最好能禁用该选项，或者至少设置为“提示”。这主要是为了防止诈骗，例如，有人非法篡改了银行网站的页面，在银行的加密页面上插入了一张来自其他位置的图片，图片的内容则是建议用户打某个电话，告知自己的账户信息。如果是这种情况，在禁用该选项的情况下根本看不到这样的图片；而就算设置为“提示”，我们至少也会知道当前页面上有来自外部站点的内容。

对于该对话框，还需要注意不同选项产生的效果。如果单击“是”按钮，此时网页将照常加载，但所有来自未加密服务器的数据都不会显示出来，此时网页的内容并不完整，但所显示的内容都是安全的；如果选择“否”，网页照常会加载，并且所有来自为未加密服务器的内容也会一起显示出来。

（35）其他/允许 Meta Refresh。

Meta Refresh 是 HTML 语言中的一个功能，可以让网页以固定的时间为间隔自动刷新。一些新闻站点经常会这样做，这样如果用户打开了自己的页面，长时间没有刷新，网页就

可以自动刷新，确保用户可以直接看到最新的新闻。

如果觉得这个功能干扰了自己的正常操作，或者不想使用这个功能，则可以将其禁用。注意，该选项只能禁用通过标准 HTML 语言中的 Meta Refresh 功能实现的自动刷新，如果浏览的网页是通过脚本或者其他方式自动刷新的，那么将不受该选项的控制。同时禁用该功能可能会影响到一些论坛或者网页本身正常的自动跳转功能。

（36）其他/允许 Microsoft 网页浏览器控件的脚本。

网页浏览器控件是一种特殊的程序，主要是为了给其他程序添加浏览网页的功能。例如，假设某个程序的开发人员希望自己的程序可以直接在程序本身的窗口中显示网页，例如显示来自官方网站的更新信息，则可以借助网页浏览器控件实现。

该选项决定了是否允许使用这种控件。为了安全起见，建议将其禁用。除非某个特定的程序确实需要该功能的时候才启用。

（37）其他/允许网页使用活动内容受限协议。

该选项决定了是否对不同的安全区域限制对活动内容的使用，该功能需要配合组策略一起使用，一般用户可以使用默认设置。

（38）其他/允许网站打开没有地址或状态栏的窗口。

有时候，一些网页经过特殊的设计可以打开不包含地址栏以及状态栏的窗口，这样做主要是为了隐藏网页地址或者其他不需要的信息，例如，在观看在线视频或者在线培训的网站上可能会遇到这种情况。

然而这种功能也容易被滥用，例如，恶意网站弹出一个没有地址栏和状态栏的 Internet Explorer 窗口，同时窗口中的内容模仿成 Windows 程序的正常窗口，诱骗我们点击其中的内容。因此，建议对该选项使用默认的“禁用”设置。

（39）其他/允许由脚本初始化的窗口，不受大小和位置限制。

为了实现一些特殊的功能，有时候网页上弹出的窗口可能会使用预先设置好的大小或者位置，例如，全屏显示或者出现在屏幕上的某个特定位置。如果不喜欢这种功能，可以对该选项使用默认的“禁用”设置。

（40）其他/在 Iframe 中加载程序和文件。

该选项决定了是否允许网页在内嵌的子框架中运行程序或文件。因为该功能可能被恶意网站滥用，因此，建议使用默认的“提示”设置，或者直接禁用。

（41）其他/桌面组件的安装。

该选项决定了是否允许网页给用户的桌面上放置快捷方式或者其他文件。基于安全方面的考虑，该选项应该使用默认的“提示”设置，或者直接禁用。

（42）启用.NET Framework 安装程序。

该选项决定了是否允许安装.NET Framework，建议使用默认的“启用”设置。

（43）下载/文件下载。

该选项决定了是否允许下载文件，默认的“启用”表示允许文件下载。如果不希望下

载文件，也可以选择“禁用”。

（44）下载/文件下载的自动提示。

该选项决定了当用户打算下载文件的时候，是否弹出允许用户直接“打开”或者“另存为”的对话框，建议使用默认的“禁用”设置。

（45）下载/字体下载。

该选项决定了如果网页上使用的某个字体在本机中没有安装的时候，是否可以自动下载并安装所需的字体。该选项请保持默认设置。

（46）用户验证/登录。

该选项决定了网页需要用户表明身份的时候使用哪种方法对待。在老版本 Internet Explorer 中，每当网页需要用户表明身份时，Internet Explorer 都会首先使用用户的 Windows 账户的用户名和密码登录，如果失败，才提供其他选项。有些恶意网站正是看准了这一点，专门编写一些需要表明用户身份的网页为套取用户的 Windows 账户密码。

该选项可供选择的设置包括：

- **匿名登录** 优先考虑使用匿名账户当做自己的身份。
- **用户名和密码提示** 提示用户输入自己的用户名和密码。
- **只在 Intranet 区域自动登录** 只有在访问 Intranet 区域的站点时才自动使用 Windows 账户表明自己的身份。
- **自动使用当前用户名和密码登录** 自动使用当前用户的用户名和密码完成身份验证（这也是老版本 Internet Explorer 的默认行为，不推荐选择该选项）。

窍门 合理利用 Internet Explorer 的安全区域

上文介绍了很多与 Internet Explorer 安全性有关的设置，那么这就可能遇到一个问题：为了访问特定的一个网站，必须启用某项设置，而启用后会降低 Internet Explorer 的安全性。这种情况下是否有比较好的解决方法？其实可以使用不同的安全区域。例如，假设需要访问的某一特定网站要求使用较低安全性的设置，但只有一个或少量我们信任的网站才需要这样的设置，那么可以将这些网站全部添加到可信站点区域，然后针对可信站点区域降低安全性。这样在访问特定网站时，可以正常使用网站的所有功能。而访问其他所有的网站时，因为这些网站都位于“Internet”区域中，因此，并不会受到可信站点区域设置的影响，依然可以获得最高程度的保护。

3. 隐私

“Internet 选项”对话框的“隐私”选项卡主要用于设置和 Cookie 以及弹出窗口阻止程序有关的设置，其界面如图 9-16 所示。

图 9-16　IE 的隐私保护选项

首先可以使用“设置”滑块为所有位于 Internet 区域的站点设置统一的隐私设置，随着滑块放在不同的位置，相应设置级别的描述信息会出现在右侧。我们可以根据实际情况选择适合的选项。

另外有一些额外的要求，例如，对于某个站点的 Cookie 总是接受，或者对于某个站点的 Cookie 总是不接受，而不用估计全局设置。因此，可以在为 Internet 区域设置了合适的保护级别后，单击“站点”按钮，随后可以看到图 9-17 所示的“每个站点的隐私操作”对话框。

首先在“网站地址”文本框中输入目标网站的地址，如果希望总是允许来自该站点的 Cookie，请单击“允许”按钮；如果希望总是禁止来自该站点的 Cookie，请单击“阻止”按钮。对于已经添加的站点，使用“删除”或“全部删除”按钮可以将其删除。

另外，在图 9-16 所示的“隐私”选项卡中单击“高级”按钮后，可以看到图 9-18 所示的“高级隐私设置”对话框。

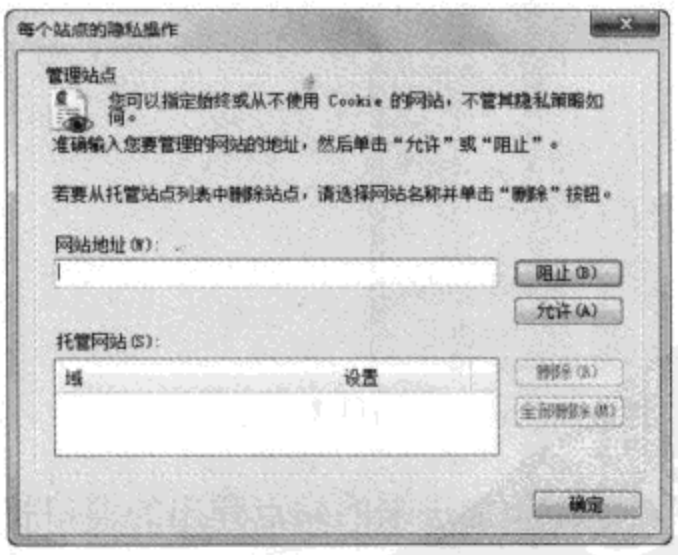


图 9-17　针对特定的站点设置隐私选项

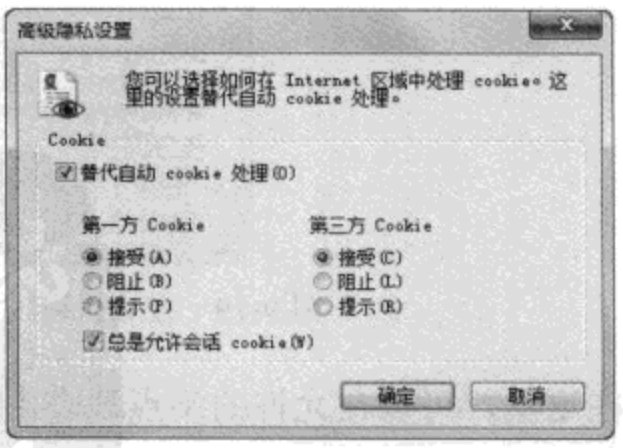


图 9-18　在这里可以设置高级隐私策略

首先，选中“替代自动 Cookie 处理”选项，随后可以针对第一方 Cookie 和第三方 Cookie 设置不同的操作。最后，还可以根据需要决定是否允许会话 Cookie。

窍门 “第一方”和“第三方”分别指谁；会话 Cookie 又是什么

其实这两个代词在不同的情况下代表的对象各不相同。例如，假设我们在访问 A 网站的页面，而 A 网站上放置了来自 B 网站的内容，同时 B 网站试图在我们访问 A 网站的时候给我们的硬盘上写入 Cookie。在这个过程中，A 网站就是“第一方”，B 网站是“第三方”。建议阻止第三方的 Cookie，因为很多网站都会使用专门的广告发布公司在自己网站上投放广告，这样广告发布公司相对我们来说就是“第三方”，而广告发布公司的 Cookie 有什么作用？自然是追踪自己的访问记录，窥探我们的隐私。

至于会话 Cookie，则是一种比较“短命”的 Cookie。正常情况下，Cookie 都有数月甚至数年的寿命，这里所说的“寿命”，表示 Cookie 的有效期。例如，假设一个 Cookie 宣告自己将于某个日期过期，那么在这个日期到达前，该 Cookie 都是有效的，可以被创建该 Cookie 的网站反复使用。而会话 Cookie 则是一种特殊的 Cookie，只有在对应会话存在的时候才会有效，一旦会话中断（例如关闭了 Internet Explorer 窗口），这种 Cookie 就会立刻失效。

在“Internet 选项”对话框的“隐私”选项卡中还可以对弹出窗口阻止程序进行设置。首先，如果想要使用这个程序，必须选中“启用弹出窗口阻止程序”选项，随后可以单击“设置”按钮对该功能进行配置。

单击“设置”按钮后，可以看到图 9-19 所示的“弹出窗口阻止程序设置”对话框。

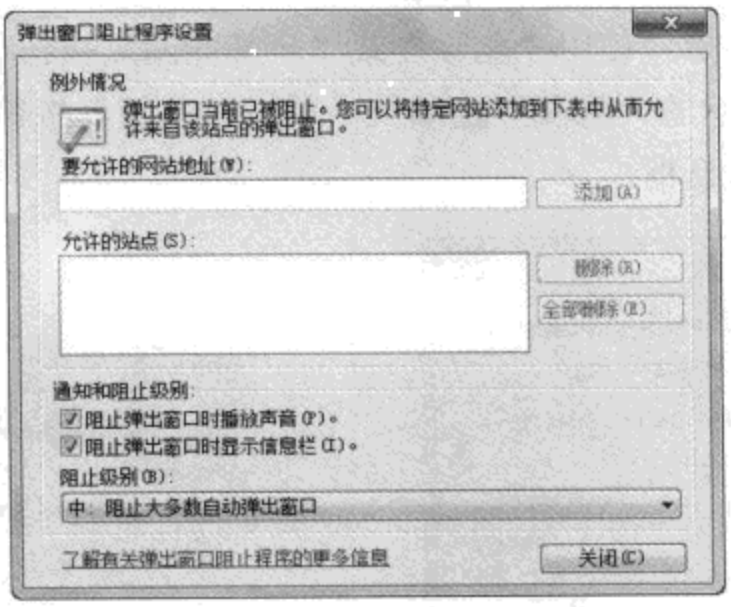


图 9-19　在这里可根据弹出窗口拦截功能进行详细设置

在这里，可以在允许的站点列表中添加站点，这样添加进来的站点弹出的窗口将会被自动打开。在“要允许的网站地址”文本框中输入站点的地址，然后单击“添加”按钮即

- android与iphone及ipad开发书籍 ----------持续不断更新中.....
- c、c++、c#语言pdf书籍及vip视频教程 c、c++、c#、vc等-------持续不断更新中.....
- delphi《书籍》及《视频》教程 ----------持续不断更新中.....
- E网情深VIP系列视频教程 黑客破解菜鸟修练班，VB编程学习班，仿站学习培训，免杀培训，个人系统攻防系列教程，服务器搭建学习班，PHOTOSHOP平面设计班，基础制作论坛（论坛网站搭建），网赚系列教程，网站建设教程，网站漏洞基础，远程控制教程，软件破解班，脚本漏洞提权班
- IT9网络学院VIP系列视频教程 免杀培训班，VMware虚拟机，零基础学习C语言，网游外挂开发精品系列语音教程（外挂教程学习必备研修31课全），VB语言教程30课全，Delphi编程到精通，远程控制软件，加密解密班，网络安全与黑客攻防培训，从入门到精通完整系统化学习C++编程，从入门到精通零基础学习汇编，wordpress教程(个人博客系统49课全)，外行人做易语言盗号和钓鱼程序语音教程 网址：WLSAM168.400GB.COM
- Java书籍 ----------持续不断更新中.....
- photoshop、CorelDRAW、AutocAD等图像处理书籍及vip视频教程 -------持续不断更新中.....
- powerbuilder书籍大全
- Visual Basic语言vip视频教程及pdf书籍 ----------持续不断更新中.....
- windows、linux系统开发、系统封装等pdf书籍及VIP视频教程 ----------持续不断更新中.....
- 《3DS Max》pdf书籍
- 《汇编语言》、《反汇编》及《调试》pdf书籍及vip视频教程 ----------持续不断更新中.....
- 《电子书、电子书、还是电子书》pdf专题库 编程开发，家居美食，儿童益智，人物传记，增强记忆，快速阅读
- 信息系统项目管理师、网络工程师、系统分析师等软考类书籍
- 华中红客系列vip视频教程 脚本攻防培训班，源码免杀培训班，Css语言培训班，C语言，Dreamweaver网页设计，html网页设计培训班，PC安全班， php脚本语言培训班，VMWare虚拟机专题，webshell提权培训班，防站教程，零基础免杀培训班，刷钻速成班，脱壳破解班，外挂编写班，网络赚钱培训班，网站入侵培训班
- 外挂、驱动、逆向及封包视频教程 郁金香、独立团、夜猫论坛、天都吧、看流星论坛、一切从零开始等等
- 安全中国系列vip视频教程 易语言软件编程培训班，ASP.net网站开发项目实战培训班
- 我的收藏
- 按键精灵及TC脚本开发软件视频教程 ----------持续不断更新中.....

当前位置：/《电子书、电子书、还是电子书》pdf专题库

文件名 ⇕

PDF电子书专题库，内容详尽，每天不断更新！！

- 办公类软件使用指南
- 医学
- 历史人物传记
- 哲学宗教
- 外语资料（除英语外） （除英语外）
- 官场类小说
- 建筑工程类
- 情感生活类小说
- 政治军事
- 教育学习科普大全
- 文学理论
- 智力开发、增强记忆、快速阅读技巧大全
- 社会生活
- 科学技术
- 程序编程类
- 经济管理
- 网络安全及管理
- 网赚系列
- 美食小吃烹饪煲汤大全
- 课外读物

本网盘内容太多，持续不断更新，发布各类视频教程、pdf书籍，包括破解、加解密、外挂辅助制作，易语言培训教程、编程语言、网页制作等等，教程及书籍仅用于学习,如用于商业或非法用途的后果自负！

网址：WLSAM168.400GB.COM

- VIP培训教程，易语言黑月VIP视频教程，天都网易语言系列培训教程(100集全)，集中营易语言学习视频(80集)
- 棉猴系列vip视频教程 gh0st远控控制源码讲解教程，套接字编程，DLL程序编写，键盘监听驱动程序编写，驱动基础教程，AsyncSelect模型QQ程序教程，C++语言入门基础，NB5.5源码分析教程
- 游戏开发pdf书籍 ----------持续不断更新中.....
- 炒股投资pdf书籍及视频教程 短线高手系列，短线天王系列，操盘论道系列，翻倍黑马，看盘快速入门，庄家手法大曝光等等。 网址：WLSAM168.400GB.COM
- 热门小说集中营 傲世九重天，网游之三国时代，武动乾坤
- 甲壳虫VIP教程全集 asp教程，Delphi培训班，FLASH培训班，Java培训班，linux培训班，PHP培训班，源码免杀班，甲壳虫C++，脚本功防班，免杀班初、中、高级班，破解班，源码免杀班，脱壳班，易语言培训班，无特征码免杀，网站架构培训班，外挂高级班，外挂初级班第1、2部
- 破解、免杀、入侵、脱壳、攻防及漏洞分析系列VIP视频教程（80多部） 天草、黑客动画吧等等--------持续不断更新中....
- 网站建设相关的pdf书籍及各种vip视频教程 ----------持续不断更新中.....
- 网赚、淘宝系列vip视频教程 网赚30天新人魔鬼训练，屠龙网赚团队vip课程，站长大学网赚视频（50课全），图腾团队日赚1000元竞价行销教程，屠龙团队淘宝宝贝卖疯系列，站群网赚系列，淘宝开店视频，红星挂机日赚10元，百万流量系列，漂流瓶圣手全自动挂机引，贴吧邮件定向营销疯狂成交量月入万元
- 英语学习资料百科大全 不断更新。。。
- 饭客论坛系列VIP视频教程 脚本入侵班，黑客之免杀教程，易语言教程，无线网络攻防教程，入侵教程，delphi系列教程，黑客基础入门
- 黑客书籍 有关黑客、安全、加解密技术等等----------持续不断更新中.....
- 黑手安全网VIP系列视频教程 DIV+CSS网页布局，Dreamweaver教程，flsah动画教程，photoshop教程，跟我一起学C++课程，抓鸡
- 黑鹰、黑基、黑防、黑盾vip系列视频教程 破解提高班66课全，SQL注入，ASP注入教程，完完全全学会抓肉鸡，脱壳破解教程50课全，提权班，C语言特训班26讲全，黑客脚本特训班，黑客工具特训班，dedecms仿站教程，VC编写远控30课全，网页美工特训班，木马免杀特训班，驱动开发技术VIP培训班，外挂破解等等。

- [电脑世界的通关密语：电脑编程基础].(杉浦贤).滕永红.扫描版.pdf
- [程序语言的奥妙：算法解读（四色全彩）].(杉浦贤).李克秋.扫描版.pdf
- [差错：软件错误的致命影响].(帕伯斯).邝宇恒等.扫描版.pdf
- [算法之道（第2版）].邹恒明.扫描版.pdf
- [O'Reilly：深入学习MongoDB].(霍多罗夫).巨成等.扫描版.pdf
- [深入浅出WPF].刘铁猛.扫描版.pdf
- [Go语言·云动力（云计算时代的新型编程语言）].樊虹剑.扫描版.pdf
- [精通.NET互操作：P/ Invoke、C++ Interop和COM Interop].黄际洲等.扫描版.pdf
- [编程的奥秘：.NET软件技术学习与实践].金旭亮.扫描版.pdf
- [O'Reilly：学习OpenCV（中文版）].(布拉德斯基等).于仕琪等.扫描版.pdf
- [Go语言编程].许式伟等.扫描版.pdf 网址：WLSAM168.400GB.COM
- [MySQL技术内幕：SQL编程].姜承尧.扫描版.pdf
- [Tomcat权威指南（第2版）].(布里泰恩等).吴豪等.扫描版.pdf
- [Ext江湖].大漠穷秋.扫描版.pdf
- [IT名人堂·Oracle DBA突击：帮你赢得一份DBA职位].张晓明.扫描版.pdf

Total: 77 1 2 3 4 5 6 ›

可。如果想删除已经添加的站点，请在选中目标站点后单击“删除”或“全部删除”按钮。

同时，还可以对弹出窗口阻止程序的一些行为进行设置。默认情况下，当有弹出窗口被拦截后，Internet Explorer 将会播放一段声音，如果不希望听到这个声音，请取消对“阻止弹出窗口时播放声音”选项的选择。另外，默认情况下，如果有弹出窗口被阻止，那么 Internet Explorer 的地址栏下方将会显示一个黄色的信息栏，提醒我们注意，并提供打开被阻止窗口的选项。如果不希望看到这个信息栏，请取消对“阻止弹出窗口时显示信息栏”选项的选择。

最后，在“筛选级别”下拉菜单中还可以决定弹出窗口阻止程序的敏感程度，只要从下拉菜单中选择相应的选项，然后单击“关闭”按钮即可。

4．内容

“Internet 选项”对话框的“内容”选项卡如图 9-20 所示，在这里主要可以设置和网页内容有关的选项，其中有不少可以影响到 Internet Explorer，甚至 Windows 的安全性。

家长控制是 Windows 7 中的一项功能，在 Internet Explorer 方面，主要控制孩子可以浏览的网页类别、是否允许下载文件等。有关家长控制功能的详细信息，请参考本书第 11 章。

内容审查程序功能则是家长控制功能的一个子集，主要可以用于决定允许浏览哪些内容的页面。该功能可以适用于任何安装了 IE 的 Windows 系统。要想使用内容审查功能，请按照下列步骤操作：

STEP 01 在图 9-20 所示的“内容”选项卡中单击“启用”按钮，打开图 9-21 所示的“内容审查程序”对话框。

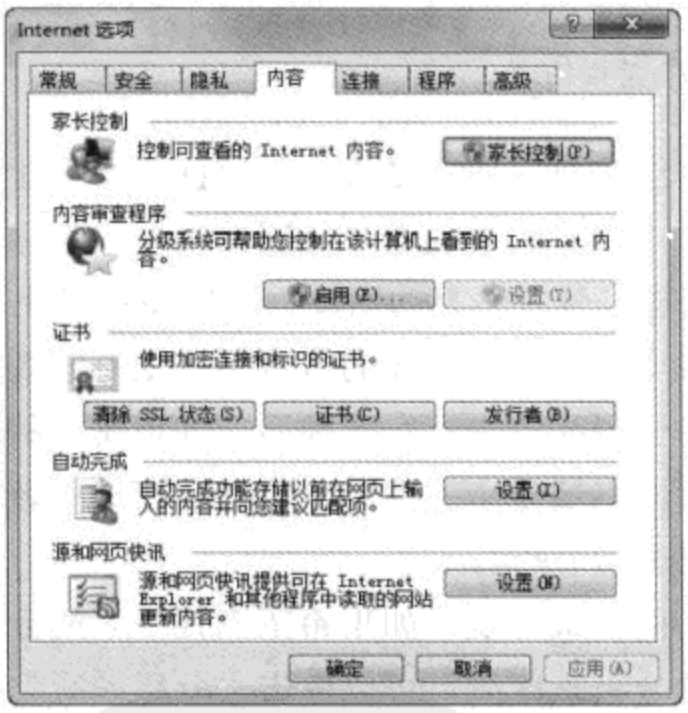


图 9-20　在这里可对 IE 的内容选项进行设置

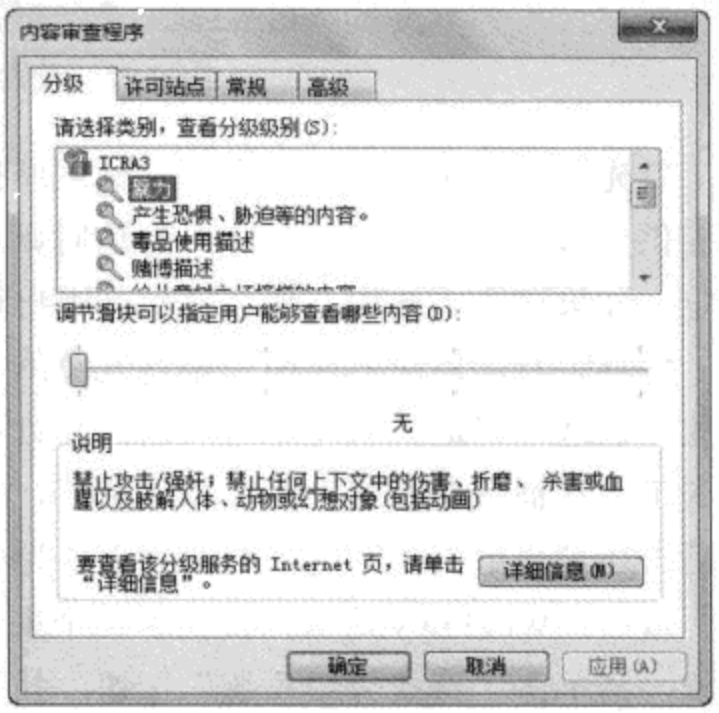


图 9-21　针对内容审查程序进行设置

STEP 02 Internet Explorer 中内容审查功能使用了来自 IRCA 的分级审查系统，因此，需要在 IRCA3 节点下分别单击选中不同的内容类别，然后拖动滑块选择一种限制级别。需

要注意的是，对于每一种需要限制的类别，都需要分别单击选中，然后拖动滑块进行设置。取决于所选类别的不同，每种类别可以限制的级别也会略有不同，请仔细查看相应类别的说明文字，然后根据实际需要设置不同的级别。

STEP 03 我们可能需要对一些站点禁用内容审查功能，这时候可以打开“许可站点”选项卡，在“允许该网站”文本框中输入站点的地址，然后单击“从不”按钮，这样无论内容审查功能是如何设置的，“从不”站点的内容都不会受到审查。当然，如果输入站点地址并单击“始终”按钮，表示无论如何设置内容审查功能，“始终”站点都会受到审查。

STEP 04 在“常规”选项卡下可以看到如图 9-22 所示的内容，在这里可以对整个内容审查功能的“常规”选项进行设置。

图 9-22　设置审查程序的常规选项

首先，内容审查程序是根据目标网站提供的分级信息来决定是否允许访问的，对于没有提供分级信息的站点该怎么办？这时候可以通过“用户可以查看未分级的网站”选项来决定，如果选中该选项，那么就允许用户查看没有提供分级信息的网站，否则将被禁止。

内容审查功能主要是用于限制儿童的，对于成年人，进行这样的审查不是很有必要，因此，在选中“监护人可以输入密码允许用户查看受限制的内容”选项后，知道密码的成年人可以在被审查系统拦截后输入密码，继续查看原本被禁止的内容。当然，在选中该选项后，还需要单击“创建密码”按钮，为成年人创建一个密码。

最后，Windows 默认只提供了一个来自 IRCA 的分级系统，如果希望查找更多的分级系统，请单击“查找分级系统”按钮。找到相应的分级系统后，可以单击“分级系统”按钮将其安装到系统中，并可以在已经安装的多个不同分级系统之间切换。

内容审查程序的设置基本上就是这些内容，该功能在国内的应用不会很广泛，因为该功能主要依靠网站主动提供分级信息，而国内因为缺乏相应的制度，几乎没有网站会主动提供分级信息。因此，无论选择哪种分级系统，在过滤国内网站方面都不会有太大的效果。

在“Internet 选项”对话框的“内容”选项卡中单击“自动完成”选项下的“设置”按钮后，可以打开“自动完成设置”对话框，在这里可以决定允许 Internet Explorer 保存哪些内容，不允许保存哪些内容。而如果希望删除这些保存的内容，请参考 9.1.1.1 节中“常规”一段的内容。

5．程序

在“程序”选项卡下，和安全有关的操作是管理加载项，因此，可以在这里直接单击“管理加载项”按钮，打开图 9-23 所示的“管理加载项”对话框。

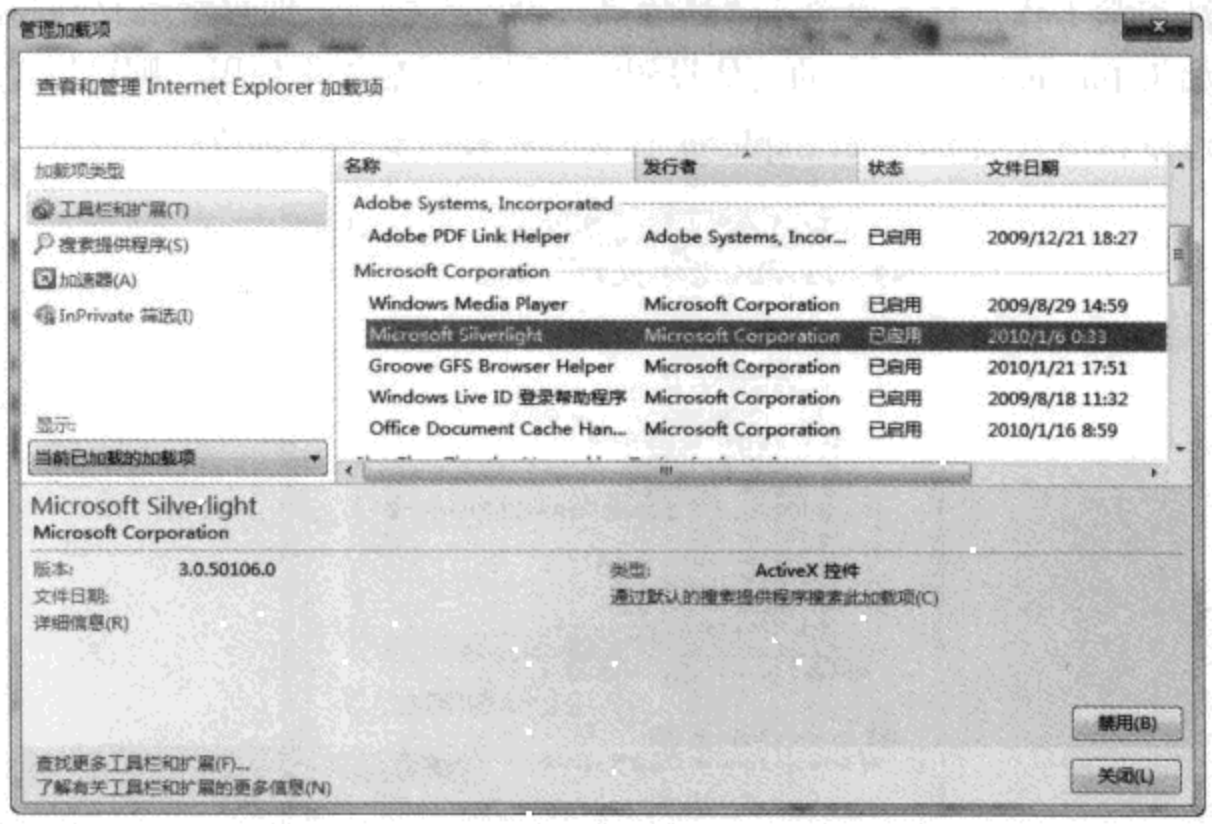


图 9-23　查看和管理系统中已经安装的加载项

首先需要注意的是，对话框左侧中央的“显示”下拉菜单，通过在这里选择不同的选项，可以按照更加合理的视图只显示自己需要的加载项，这里提供的选项如下：

- **当前已加载的加载项**　该选项可以显示当前 Internet Explorer 正在使用（已经加载）的加载项。
- **所有加载项**　该选项可以显示 Internet Explorer 中已经安装的所有加载项（无论当前是否被加载）。
- **未经许可运行**　该选项可以显示一些预设的或者被直接信任的加载项。
- **已下载控件**　该选项可以显示通过网页下载并安装的加载项。

为了管理所有的加载项，可以选择“所有加载项”，随后所有符合条件的内容就会显示在下方的列表中。在列表中单击加载项后，可以通过“启用”和“禁用”按钮将其启用或者禁用。如果被选中的加载项可以被直接删除，那么还会出现“删除”按钮，单击它，即可将所选的加载项删除。

对于加载项，本书的建议是，如果不知道某个加载项有什么作用，或者如果觉得某个

加载项的信息有些可疑，那么最好立刻将其禁用，如果有必要，还可以将其删除。

如果 Internet Explorer 因为某些加载项导致已经无法启动，那么还可以在“开始”菜单的“附件”→“系统工具”子菜单下单击“Internet Explorer（无加载项）”，启动安全模式的 Internet Explorer，并禁用或删除怀疑可能导致 Internet Explorer 无法正常启动的加载项。

6. 高级

在“Internet 选项”对话框的“高级“选项卡下有很多设置，不过本节主要介绍“安全”类别下的选项（如图 9-24 所示）。注意，如果因为“高级”选项卡下的设置错误导致 Internet Explorer 无法正常工作，只需要单击“还原高级设置”按钮，即可将所有的高级设置恢复为默认值。如果 Internet Explorer 的其他设置错误导致无法正常使用，则可以单击“重置”按钮，这样可以将所有和 Internet Explorer 有关的设置恢复为默认值。

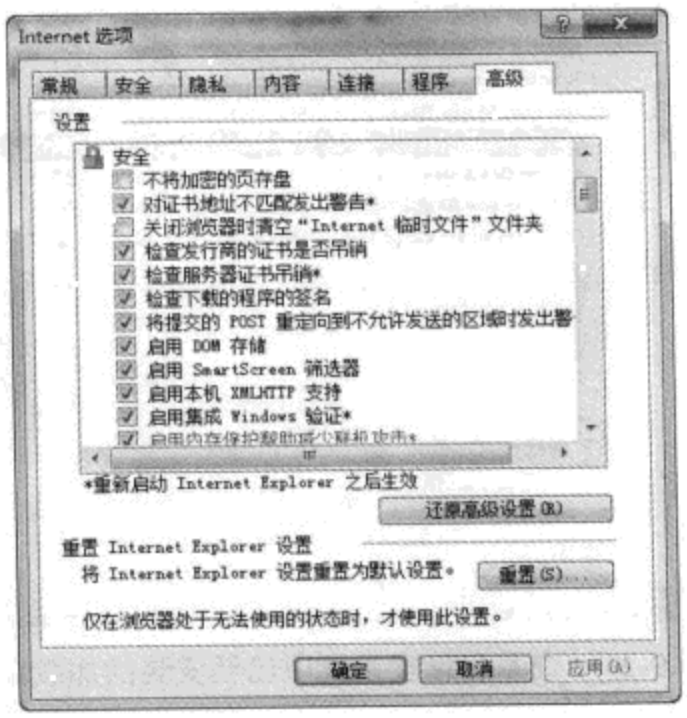


图 9-24　IE 的“高级”选项

（1）不将加密的页存盘。

该选项决定了是否允许将加密的网页内容保存在硬盘上，该选项的默认设置是“禁用”，一般情况下也没必要启用该功能，除非是企业网络内部的管理员不希望员工将内部加密服务器上的网页保存下来。

（2）对证书地址不匹配发出警告。

该选项默认是被选中的，这样，当我们试图访问一个安全站点（地址以“https”开头）的时候，Internet Explorer 会自动检查该站点提供的加密证书是否符合站点的地址。例如，假设一个网站提供的加密证书表示该证书是颁发给“www.site.com”的，而我们访问所用的地址是“https://site.com”，虽然这两个地址可以理解为同一个网站，但如果选中该选项，Internet Explorer 会对我们发出警告。

当然，该选项更多情况下是用于增强安全，防范钓鱼网站使用颁发给其他网站的证书

创建伪造网站，因此，不建议修改该选项的默认值。有关该选项的详细信息，请参考 9.1.2.1 节加密网站甄别。

（4）关闭浏览器时清空“Internet 临时文件”文件夹。

如果有很多人共用一台计算机，那么最安全的做法是给每个人创建自己独立的用户账户，并使用密码保护每个账户。这样每个人使用自己的账户登录系统，同时 Internet Explorer 浏览网页过程中生成的临时文件、Cookie、历史记录等包含了个人隐私的数据就会保存在每个账户的配置文件中，不同账户之间不会造成泄露。

如果因为某些原因，只能很多人共用一个账户，这些人可能习惯于在上网之后手工删除所有的历史记录。虽然 Internet Explorer 中新增的功能可以让我们在一个统一的界面中删除所有的隐私数据，不过有时候可能会有人遗忘。因此，更好的办法是选中该选项，这样，当关闭所有的 Internet Explorer 窗口后，Internet Explorer 会自动删除这些信息。注意，该选项默认并没有被启用。

（5）检查发行商的证书是否吊销。

当使用 Internet Explorer 下载了一个程序的安装文件后，默认情况下，Internet Explorer 会自动检查该安装文件是否带有数字证书，以证明开发商的身份，并证明文件没有被恶意篡改。

这本是很好的功能，但有时候可能会有这样的情况：某个软件开发商申请了一个用于给程序进行签名的数字证书。然而一旦因为一些原因，例如程序开发商保存的私钥被盗，窃贼可能会使用偷来的私钥在自己开发的病毒或者间谍软件中添加数字证书，这样在用户看来，下载的软件带有这家软件公司的签名，可以放心安装，但实际上这是窃贼利用偷窃来的证书伪造出来的。为了防范这种问题，一旦私钥丢失，私钥的持有人可以向证书颁发机构申请吊销证书，这样虽然被窃的证书依然可以用来对文件进行签名，但因为已经被吊销，因此，是不被信任的。

如果选中该选项(默认值)，Internet Explorer 不仅会检查下载的文件是否包含数字证书，还会验证数字证书是否依然有效。一旦检测到证书是被吊销的，那么就会警告用户。

（6）检查服务器证书吊销。

该选项的含义和上一个选项类似，只不过上一个选项适用于下载回来的软件中包含的数字证书，而这个选项适用于访问加密网站时网站提供的证书。

（7）检查下载的程序签名。

当我们使用 Internet Explorer 从网上下载了可执行文件，并运行的时候，Internet Explorer 首先会检查文件是否包含数字证书，并显示图 9-25 所示的界面。

如果检查发现要运行的可执行文件包含有效的没有被吊销的数字证书，那么在“已验证的发布者”一栏将可以看到该程序的开发公司的名称；如果检查发现要运行的可执行文件不包含数字证书，那么图 9-25 所示的对话框会用红色的背景提醒注意，这种情况很可能是因为文件本身不带数字证书，或者虽然带有数字证书，但文件在签名后被篡改过，导致

证书失效。

图 9-25　运行 IE 下载的文件时系统会检查数字证书

这是一个很好的功能，并且默认是启用的，它可以帮助我们判断下载的文件是否可信，但也存在一些问题。例如，如果下载回来的文件很大，那么检查证书所用的时间就会很长，而且很多安全意识不强的公司都没有给自己提供的文件添加数字签名的习惯。因此，如果觉得这个功能严重影响了系统的运行速度，可以禁用该选项，不过不推荐这样做。

（8）将提交的 POST 重定向到不允许发送的区域时发出警告。

在上文“其他/提交非加密表单数据”一节中曾介绍过，通过这个选项可以决定，当我们要提交文本内容的网页没有使用加密技术的时候，是否允许提交。

这里可能存在这样的情况：我们对某个安全区域（例如，受限站点区域）设置禁止提交，当前访问的是 Internet 区域的站点 A。然而该站点会将我们提交的信息转发到一个位于受限制站点区域中列出的站点 B 上。这种情况下，如果启用了该选项，那么 Internet Explorer 会提醒我们注意；如果禁用了该选项，Internet Explorer 不会显示任何警告信息。当然，无论这个选项选择的是什么，因为我们针对站点 B 所在的受限站点区域已经设置了禁止提交，因此，自己的数据无论如何是不会被提交上去的，而这个选项只是决定了是否在我们按照上面提到的方式提交数据的时候发出警告。

（9）启用 DOM 存储。

DOM 存储是从 Internet Explorer 8 开始增加的一项功能，该功能可实现类似 Cookie 的特性，在客户端中存储与特定会话或特定域有关的信息。关于 DOM 存储的详细介绍，可参考 http://tinyurl.com/y7yblsq。对于一般用户，该选项的意义不大，因此，可保留默认设置。

（10）启用 SmartScreen 筛选器。

SmartScreen 筛选器的用途是为了防范仿冒网站，因此，可根据情况决定是否需要使用该功能。有关该功能的详细介绍，请参考下文。

（11）启用本机 XMLHTTP 支持。

该选项决定了是否在本机启用 XMLHTTP，默认设置是启用，一般情况下不建议修改。

（12）启用集成 Windows 验证。

该选项决定了是否使用 Windows 支持的 LM、NTLM、NTLM v2，以及 Kerberos 这 4

种验证方式向网站证明自己的身份。该选项的默认值是启用，一般不建议修改该选项，因为可能会导致某些安全网站（尤其是企业内部的网站）无法访问。

（13）启用内存保护帮助减少联机攻击。

为了防范缓冲区溢出攻击，从 Windows XP SP2 开始，微软给 Windows 中增加了一个叫做数据执行保护（DEP）的功能。简单地说，该功能可以将内存中的数据标记为“可执行的”和“不可执行的”，对于标记为“不可执行”的数据，无论如何是不会执行的。以前支持 DEP 的系统中，Internet Explorer 默认并不会开启 DEP，而且 Internet Explorer 中安装的扩展也不会开启 DEP，因此，可能会导致一些安全问题。不过从 Internet Explorer 8 开始，无论是 Internet Explorer 本身，还是安装的扩展，为了提升安全性，默认都会开启 DEP，这也有可能导致一些兼容性问题（主要出现在某些 Internet Explorer 扩展中）。

另外还需要注意，该选项正常情况下是灰色的，不可选。要启用该选项，必须使用管理员身份启动 Internet Explorer（在 Internet Explorer 的快捷方式上单击鼠标右键，选择“以管理员身份运行”），同时，启用该选项可能导致某些 Internet Explorer 加载项工作异常。

（14）使用 SSL 2.0\使用 SSL 3.0\使用 TLS 1.0\使用 TLS1.1\使用 TLS 1.2。

该选项决定了允许 Internet Explorer 使用哪种版本的 SSL（Secure Socket Layer，安全套接字层），其中 TLS 是 SSL 的改进版。默认情况下，对 SSL 3.0 和 TLS 1.0 是启用的，如果不是在访问某些特殊加密网站的时候遇到问题，通常情况下不建议更改这几个选项的设置。

（15）允许活动内容在“我的计算机”上的文件中运行\允许来自 CD 的活动内容在“我的计算机”上运行。

这两个选项决定了在 Internet Explorer 中加载位于本地（前者适用于保存在本地硬盘上的内容，后者适用于保存在光盘上的内容）的活动内容时，是否允许活动内容在本机上运行，也就是说，决定了是否允许活动内容在“本地计算机”安全区域（这是一个特殊并且隐藏的 Internet Explorer 安全区域，安全设置较为宽松）的设置下运行。

例如，默认情况下，当使用 Internet Explorer 打开保存在本地的活动内容（例如网页脚本或 html 页面文件）时，可能会看到图 9-26 所示的信息，同时文件的内容可能也无法完全显示，或者文件提供的功能无法完全使用。

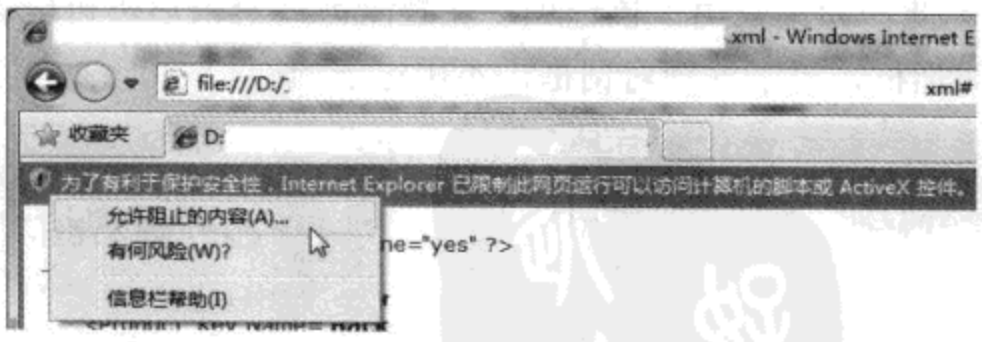


图 9-26　打开位于本地的活动内容时可能会受到限制

这种情况下有两个选择：如果只是偶尔需要这样使用，可以直接单击 Internet Explorer 窗口工具栏下方的信息栏，从弹出菜单中选择“允许阻止的内容”；如果需要经常这样做，

那么可以根据要运行的活动内容的保存位置启用对应的选项。

（16）允许运行或安装软件，即使签名无效。

在上文“检查下载的程序的签名”一段中曾经提到过，当用 Internet Explorer 从网站上下载了软件的安装程序并运行的时候，默认情况下，Internet Explorer 首先会检查该文件是否包含数字签名，以及数字签名是否有效。如果有效，就会显示一个对话框，其中列出了软件的开发商名称；如果不带签名，或者签名无效，就会用红色的对话框提醒我们注意。

可见，有两种情况会导致 Internet Explorer 用红色的对话框提醒我们注意：下载的文件根本不带数字签名，或者原本带有数字签名，但因为添加签名后文件被篡改过，导致签名无效。这两种情况中，前一种还可以接受，因为很多厂商还没有给文件添加签名的意识，但后一种问题就比较多了。

请假设这样的情况：软件公司 A 开发了一个软件，并使用自己的证书给文件添加了数字证书，证明该文件是公司 A 开发的。随后很多专门提供下载服务的网站上都可以下载到这个文件，然而某个网站的服务器中毒，导致提供下载的文件都被病毒感染，这意味着文件已经被篡改，因此，会导致文件包含的数字签名失效。而该选项则决定了是否允许运行这样带有签名，但签名失效的程序。注意，对于原本就不带签名的程序，该选项不会发生作用。

该选项的默认值是禁用，如果不是特别必要，不建议启用该选项。

（17）在安全和非安全模式之间转换时发出警告。

对于 Internet Explorer 来说，安全模式是指访问加密网站，非安全模式是指访问非加密网站。因为网页是包含超级链接或者重定向功能的，因此，我们可能在安全网页上单击了一个链接后，进入了一个非安全网站，反之亦然。而这个选项就决定了当从安全网站转向非安全网站，或者从非安全网站转向安全网站的时候，Internet Explorer 是否提示注意。

该选项默认是被启用的，不过在遇到这样的提示时不用太担心，因为这并不意味着 Internet Explorer 不安全了。例如，在某个网站上登录的时候，网站可能会将登录界面单独加密起来，但是登录后看到的网站内容依然是没有加密的。这样不仅可以保证用户输入的信息的安全，还可以避免网站投资过大（毕竟加密登录页面对应服务器的投入要比加密整个网站少多了）。因此，如果启用了该选项，在登录前或登录后，可能会看到类似图 9-27 和图 9-28 所示的对话框，对于这种对话框，不用过于担心。

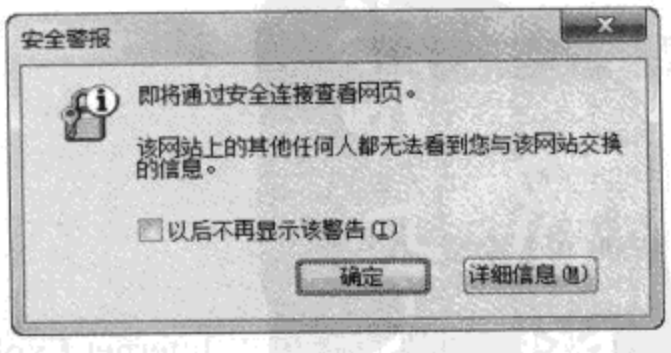


图 9-27　从不安全网页转向安全网页

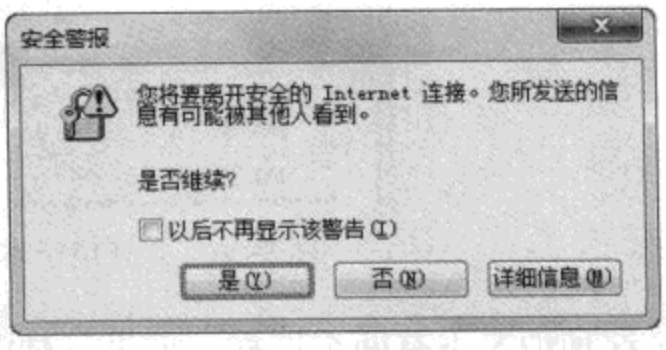


图 9-28　从安全网页转向不安全网页

如果在图 9-27 和图 9-28 所示的对话框中选中“以后不再显示该警告”，那么该选项将会被禁用。

9.1.1.2　信息栏

信息栏是从 Internet Explorer 6 SP2 开始增加到 Internet Explorer 中的一个新功能。当在 Internet Explorer 中进行的某些操作需要引起注意的时候，Internet Explorer 就会利用在地址栏下方显示的一个“长条状”的黄色工具栏提醒我们注意。

根据具体情况的不同，Internet Explorer 8 的信息栏有多种不同的表达方式，下文将列举一些最常见的信息栏以及对应的含义。

1．弹出窗口拦截

弹出窗口是指当浏览网页的时候，网页上使用特殊的脚本或其他方式在网页主窗口外另打开一个新窗口，并在其中显示内容。最初的弹出窗口是作为网站提醒访客的用途使用的，例如，网站可能会使用弹出窗口告诉访客一些有关网站的最新信息等。然而这个功能逐渐开始被滥用，主要用来显示网站上的各种广告。在弹出窗口广告最猖獗的时候，有些网站直接会弹出四五个广告窗口，不仅影响网页的加载速度，而且很烦人。

Internet Explorer 中带有弹出窗口拦截功能，当网页试图弹出窗口，并且被 Internet Explorer 拦截后，就能看到图 9-29 所示的信息栏，单击该信息栏后可以看到不同的选项。

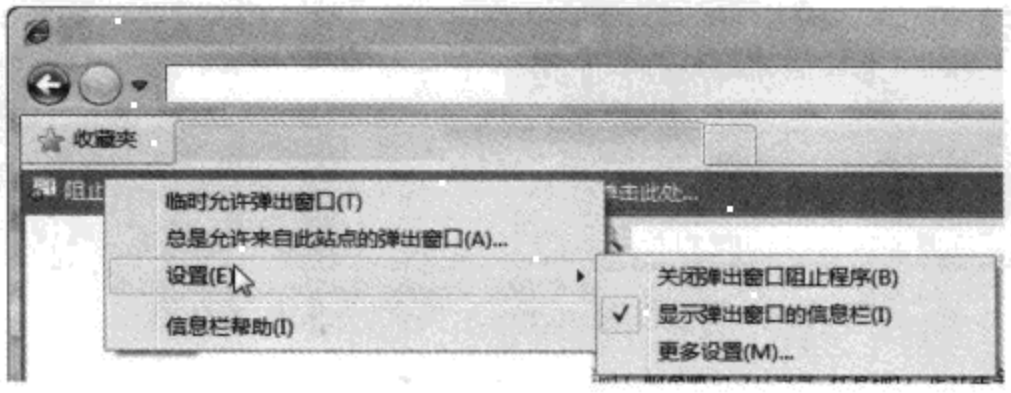


图 9-29　弹出窗口被拦截后的信息栏和相关选项

如果只是希望临时打开被拦截的弹出窗口，可以从菜单中选择“临时允许弹出窗口”，这样网页将被自动刷新，打开被拦截的弹出窗口。直到关闭 Internet Explorer 之前，该站点上的弹出窗口都会被自动打开，不会被拦截。

如果希望永远允许打开来自该网站的弹出窗口，则可以选择“总是允许来自此站点的弹出窗口”选项。

关于弹出窗口拦截功能的详细信息，请参考本章上文“隐私”一节的相关内容。

2．ActiveX 控件安装

网页最初的用途很单纯，就是给访客提供各种需要的信息。然而为了能提供越来越多的交互性，很多网站开始采用不同的技术来增加网页的功能，其中很大一部分都采用了

Internet Explorer 的 ActiveX 控件。

简单来说，ActiveX 控件就是一些通过 Internet Explorer 安装的小程序实现 Internet Explorer 原本不支持的功能。例如，在网页上看到的 Flash 动画，就是由 ActiveX 控件实现的。

可以说，ActiveX 控件的本意是好的，因为它扩展了 Internet Explorer 的功能，可以实现很多无法直接通过单纯网页实现的应用。然而一些不良的软件开发人员纷纷意识到，通过 ActiveX 控件，他们可以绕过系统对 Internet Explorer 的很多限制，实现以往单纯通过网页脚本所不能进行的操作（例如，格式化硬盘分区、窃取访问过的网络地址或者给系统中弹出广告窗口），因此，各种目的不那么单纯（至少不像宣称的那么单纯）的 ActiveX 控件问世了。

在老版本的 Internet Explorer 中，如果网页试图在系统中安装控件，Internet Explorer 会直接显示一个对话框，询问是否安装。很多人因为不明白这是什么，往往会直接单击“确定”，这样造成的结果都是很严重的。为了避免很多人对 ActiveX 控件的消极看法，从 Internet Explorer 6 SP2 开始，如果网页试图安装 ActiveX 控件，Internet Explorer 并不会直接弹出询问是否允许安装的对话框，而是显示一个如图 9-30 所示的信息栏。只有在单击这个信息栏之后才可以看到相应的选项（如果是支持 UAC 的系统，默认情况下还需要首先经过 UAC 功能的提升，这也就意味着在此类系统中的非管理员用户无法安装 ActiveX 控件）。

图 9-30　需要安装 ActiveX 控件时的 IE 信息栏

单击该信息栏后，如果打算安装这个控件，必须单击“安此加载项”选项，随后才可以看到询问是否安装的窗口。而在 Windows 7 中，ActiveX 加载项技术也有所改进，开始支持“每用户”加载项。也就是说，对于支持这一特性的加载项，可以只安装给当前用户，或者安装给本机的所有用户。

根据统计，很多直接在询问是否安装 ActiveX 控件的对话框中单击“是”按钮的用户，往往都不会注意到信息栏的存在。因此，这样的设计进一步避免了用户无意中将控件安装到系统中的危险。

3. 自动下载提示

正常情况下，如果想要从网站上下载一个文件，最常见的办法就是打开软件的下载页面，然后单击下载链接，随后 Internet Explorer 会询问我们是要直接打开文件还是保存文件。如果选择“保存”，还可以选择保存位置和希望使用的文件名。

然而有些网站（尤其是提供下载服务的网站）为了方便使用，往往会在没有单击下载链接的情况下直接主动向我们发送文件。虽然这种做法的初衷是为了方便使用，但也会带来不少安全隐患。

例如，网页会自动向访客推送一个间谍软件的安装程序，如果访客对此不了解，可能会选择直接运行该程序，或者将其保存到硬盘上。虽然也可以选择取消，但这最起码增加了一个恶意网站入侵我们系统的途径。因此，在新版的 Internet Explorer 中，如果访问的网页未经点击就主动向我们推送程序，Internet Explorer 会将其拦截，并显示图 9-31 所示的信息栏。

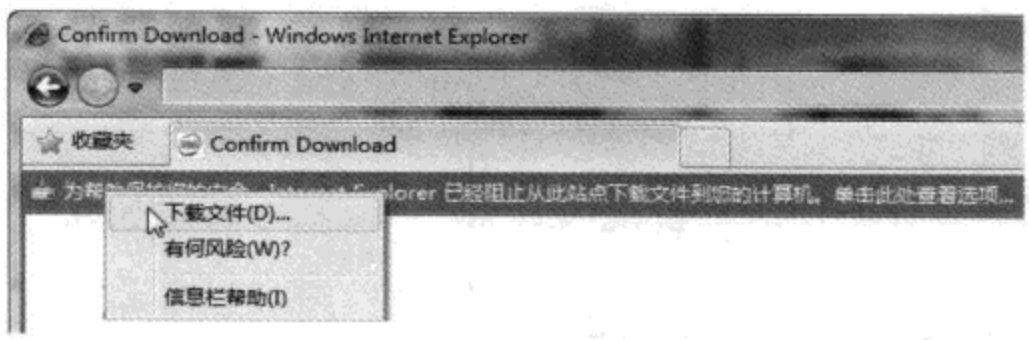


图 9-31　网页自动推送文件时的信息栏

如果需要下载这个文件，只要单击“下载文件”选项，即可刷新页面，并自动接受推送的文件。当然，该选项只对当前站点的当前访问有效。如果是在同一个网站上再次遇到推送页面，或者在其他网站上遇到推送页面，Internet Explorer 依然会询问。

4．安全性提醒

在遇到安全性问题的时候，很多人都直接怪罪于 Windows。其实安全性也存在木桶原理，也就是说，木桶能够装多少水，取决于其中最短的一块木板，而非最长的木板。同理，整个系统的整体安全性也取决于其中最不安全的组件，而非最安全的组件。

Internet Explorer 的安全性广受争议，默认设置下，Internet Explorer 8 虽然是相当安全的，但是安全性和易用性永远是矛盾的，如果提高安全性，就会降低易用性；如果提高易用性，就会降低安全性。Internet Explorer 的默认设置虽然可以保证最高程度的安全，但会在我们访问网页的时候制造不少困难。

例如，国内某银行的网络银行程序，因为自身程序的不足，无法在默认设置的 Internet Explorer 8 中正常使用，因此，在安装该银行提供的网络银行控件程序后，安装程序会询问是否调整 Internet Explorer 的默认安全设置，以便能够顺利地使用网上银行。在这种情况下，用户自身的安全性原本已经很高了，然而这家银行非但不主动提升自己软件的安全性以适应用户，反而要用户降低安全性来适应自己。尽管很多人都意识到了这一点，然而为了能正常使用网络银行业务，不得已还是得接受这种不安全的设置。

在 Internet Explorer 8 中如果遇到上述情况，怎么才能知道自己的哪些安全设置被修改了，又怎样才能用最简单的办法恢复回来？Internet Explorer 已经为我们想到了。一旦检测

到自己的某些安全设置被修改，变得不够安全，就会用图 9-32 所示的信息栏提示我们注意，同时如果单独打开一个 Internet Explorer 窗口，不加载任何网页，那么空白页面上也会出现安全性警告。另外，Windows 7 的操作中心此时也会发出警报。

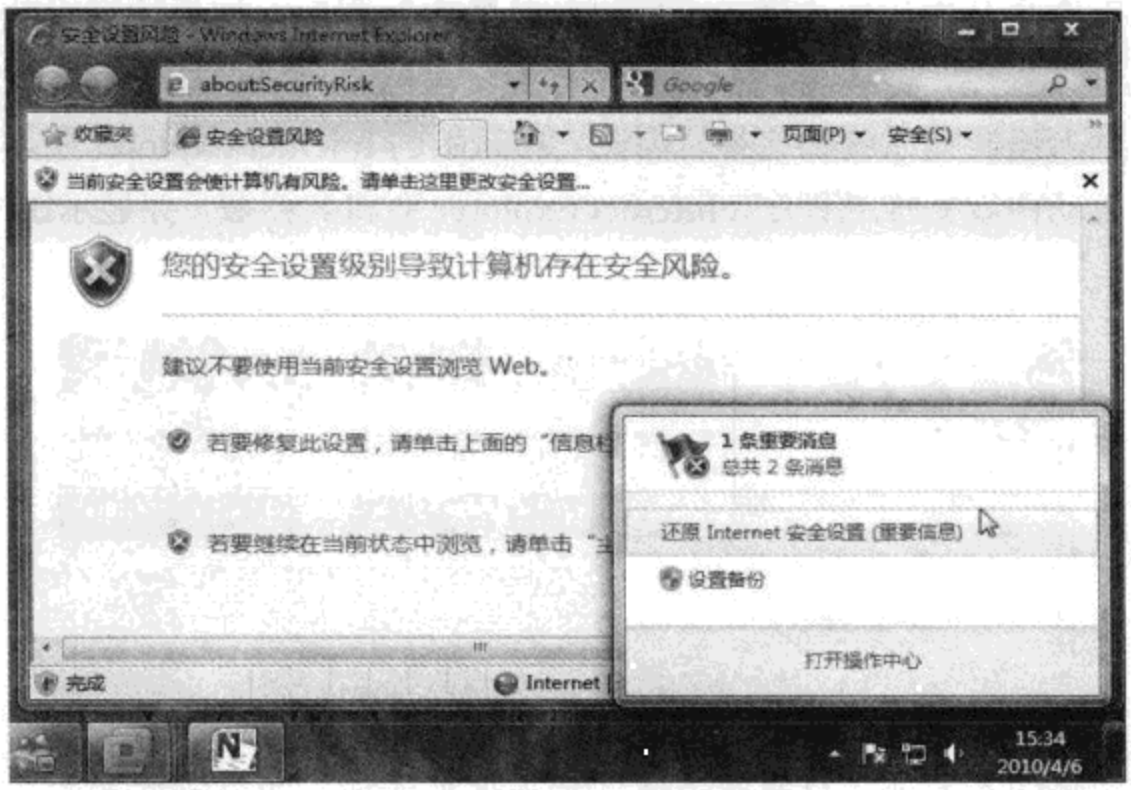


图 9-32　Windows 7 中的各种 IE 风险提示

如果不需要了解具体有哪些设置被更改，只希望用最简单的方法恢复成默认的安全设置，只需要单击信息栏，然后选择“修复设置”即可。

如果希望了解具体有哪些选项被更改，则可以选择“打开安全设置”选项，随后系统会自动打开“Internet 选项”对话框的安全选项卡，并用一个红色的“叉”图标突出将不安全的设置标示出来。同时对于具体的选项，如果设置得不够安全，那么选项的背景将会使用红色显示，提醒我们注意（如图 9-33 所示）。

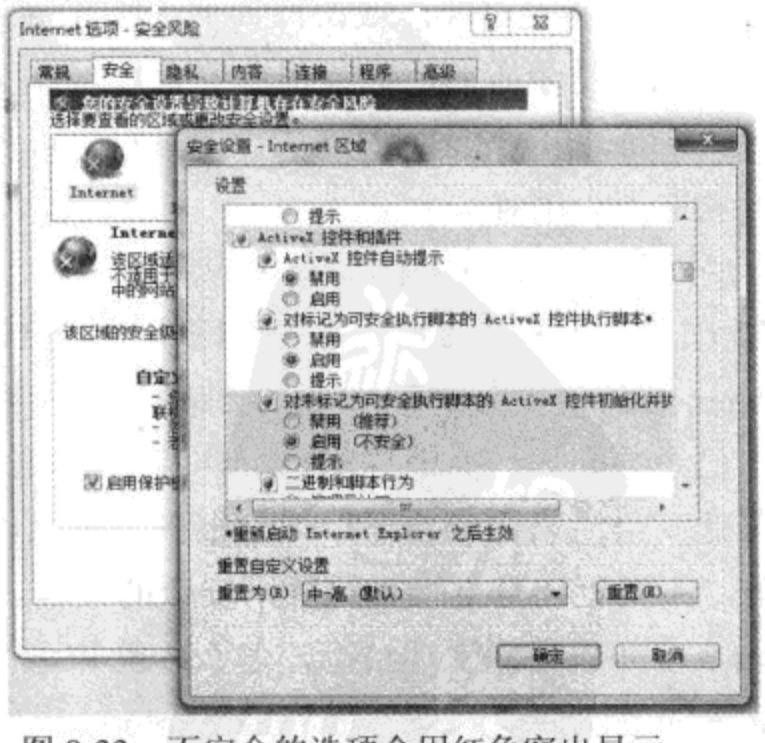


图 9-33　不安全的选项会用红色突出显示

9.1.2　Internet Explorer 的安全设置和隐私选项

除了上述的安全选项之外，Internet Explorer 还有几个安全功能是需要我们注意的。虽然这些功能默认已经被启用，不过通过适当的设置，才可以更好地符合我们的实际需要。

9.1.2.1　加密网站甄别

加密网站一般都用在很特殊的场合，例如网络交易网站，或者网络银行网站等。一般情况下，在 Internet Explorer 中可以通过下列方式判断这个网站是否是加密的：

- 在地址栏上，网页的地址以“https://”字样开头。
- 地址栏右侧显示有一个黄色的锁头图标。

如图 9-34 所示的就是用 Internet Explorer 打开一个加密网站后显示的上述所有的特征。

图 9-34　IE 中打开加密网站后的特征

对网页进行加密有两个原因：在访问加密网页的时候，浏览器和网页服务器之间的通信数据是通过证书加密后传输的，一旦有人窃取双方之间的通信数据，因为缺少证书，无法解密被加密的数据，因此，不会造成信息的泄露，同时也可以防止有人篡改浏览器和服务器之间的数据。另外一个原因是，通过加密（严格地说，这属于数字签名的范畴），我们可以判断网站是否可信，因为恶意网站就算可以伪造自己的网页，让网页和正规网站（例如银行网站）完全一样，因为没有银行的数字证书，我们可以从数字证书中获知网站的真实身份。

第一个原因很好理解，第二个原因是什么意思？让我们单击图 9-34 中地址栏右侧的锁头图标，随后可以看到图 9-35 所示的界面，通过这些信息，我们可以判断网站的真实身份。

图 9-35　服务器的证书信息

以图 9-35 中的例子来说，其中显示的“Class 3 Public Primary Certification Authority”是证书颁发机构，而“www.alipay.com”是证书持有人。那么到底应该怎样通过这些信息判断网站是否可靠？

在这里，一个很通用的规则是，如果 Internet Explorer 检测到加密网站所用的证书是正常的，那么地址栏就会显示为绿色或者白色，这种情况下可以放心地浏览该网站，并提交自己的数据；如果 Internet Explorer 检测到网站的证书有问题，那么地址栏就会显示为红色，提醒我们注意，同时取决于具体情况，地址栏右侧会显示有“证书错误”按钮，而且网站内容不会显示，取而代之的是 Internet Explorer 的警告信息。

这个过程的基本原理是：假设我们信任 A 公司，而 A 公司信任 B 公司，那么我们就可以信任 B 公司。很明显，“www.alipay.com”的证书是“Class 3 Public Primary Certification Authority”颁发的，这表示后者信任前者，可以证明前者的真实身份，但是我们又凭什么信任后者这个证书颁发机构？

> **注意** 信任的含义
>
> 上述文字里不止一次提到“信任”一词，那么“信任”在这里是什么意思？是否像我们平时讲话时说的“我信任他”那样，代表我们相信他是个好人，不会干坏事？其实完全不是这样。这里所说的“信任”，只是说明证书持有人的身份是真实可靠的，至于持有人用这个证书干什么事情，不在“信任”的范畴内。例如，网上很多臭名昭著的恶意软件，现在都带有数字证书（倒是很多正规用途的软件因为开发商缺乏安全观念不带证书），同时因为这些数字证书的“根”都是我们信任的根证书颁发机构，因此，Windows 是信任这些公司的身份的，但并不代表这些公司的软件不会干坏事。只要肯花钱，任何人都可以在商业性质的证书颁发机构买到直接被 Windows 信任的证书。

其实，Windows 中本身就包含一些受信任的证书颁发机构的证书，要查看这些根证书，可以运行“certmgr.msc”打开证书控制台，然后从控制台窗口左侧的控制台树中依次进入“证书当前用户”→“受信任的根证书颁发机构”→“证书”，随后右侧的窗口中会显示本机预置的所有根证书颁发机构，其中就有“Class 3 Public Primary Certification Authority”，这表示我们信任“Class 3 Public Primary Certification Authority”，而“Class 3 Public Primary Certification Authority”信任“www.alipay.com”，因此，我们可以信任“www.alipay.com”。如果从证书控制台中删除“Class 3 Public Primary Certification Authority”的根证书，表示我们不再信任它，那么它所信任的公司也将不再被我们信任。

> **注意** “不信任的证书”节点下为何会有微软的证书
>
> 按照上文的方法打开证书控制台，并进入到“不信任的证书”→“证书”节点后，还会发现里面列出了两个颁发给“Microsoft Corporation”的证书，为什么微软

> 自己的操作系统会不信任颁发给微软的证书？仔细检查这两个证书的“截止日期”就可以发现，这两个证书在 2002 年初就已经过期了。根据说明（参见 http://tinyurl.com/y93had2），微软无意中遗失了这两个证书对应的私钥，而获得该私钥的人可能会利用私钥将自己开发的软件伪装成微软的产品，诱骗用户安装。为了安全，微软已经在证书颁发机构撤销了这两个证书，也就是说，已经将这两个证书设置为不被信任，这主要是为了保护 Windows 用户不受骗。因此，不要因为看到证书是微软颁发的就将其删除。

这里要重点提出“根证书”这个概念，全世界具有提供数字证书业务的公司有很多，而 Windows 自带的“根证书”很少，默认情况下，我们是如何信任这么多不同公司颁发的不同证书的？其实这就是“根”这个字的含义，因为可以颁发证书的公司虽然很多，但最基本的根证书颁发机构只有有限的几个，默认情况下都是被 Windows 信任的。那么，既然 Windows 信任根证书颁发机构，自然也就可以信任被根证书颁发机构信任的公司，进而可以信任被这些公司所信任的下一级公司。

如何证明这一点？可以单击图 9-35 中的“查看证书”链接，随后可以打开“证书”对话框，切换到“证书路径”选项卡后，可以看到图 9-36 所示的界面。从该图中可以看出，整个证书信任链的路径分为三个层次，最顶层的是我们信任的根证书颁发机构，该机构给“www.verisign.com”颁发了证书，因此，我们信任“Verisign”；随后“Verisign”又给“www.alipay.com”颁发了证书，因此也可以信任“www.alipay.com”。如果“www.alipay.com”再给别人颁发证书，那么这个人的身份依然可以被我们信任。

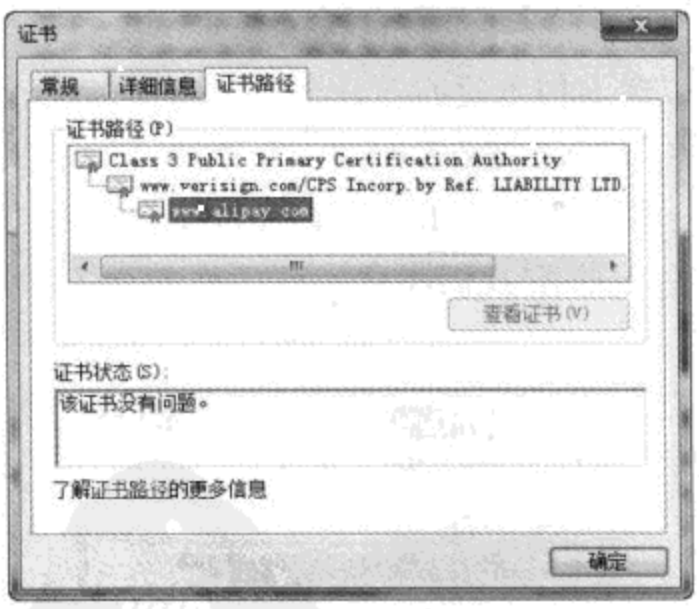


图 9-36　证书的信任链

简单介绍了加密网站的数字证书以及相关事项后，再来看看在浏览各种加密网站的时候会遇到什么状况。

1．不被信任的证书

当访问某些加密网站的时候，可能会遇到图 9-37 所示的情况。

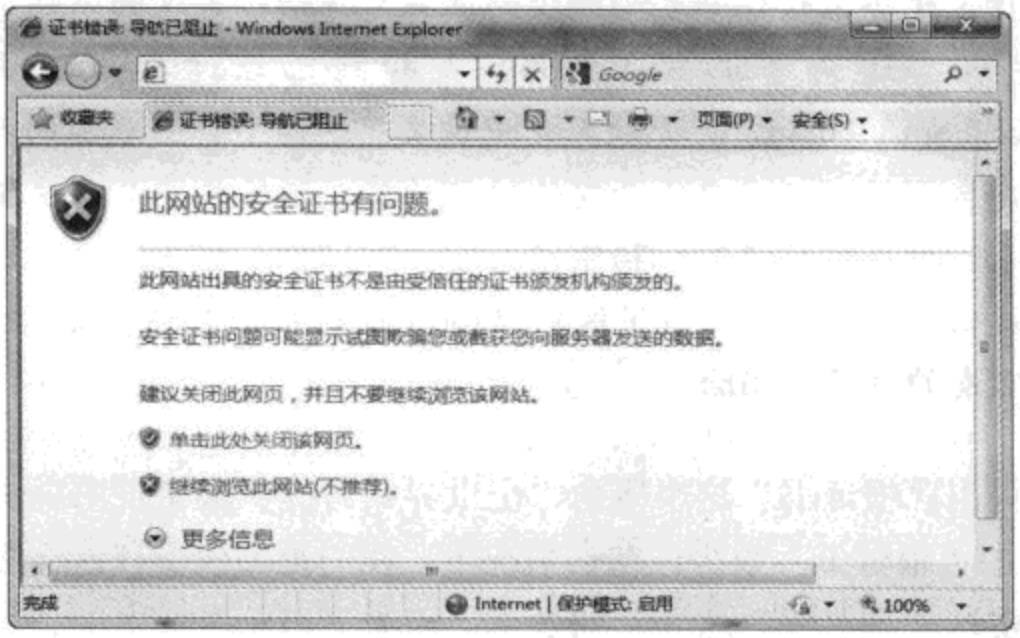


图 9-37　被访问的网站使用了不被信任的证书

发生这种问题的主要原因是：网站加密所用的证书是自己给自己颁发的，因为不是来自受信任的根证书颁发机构，因此，不被 Windows 信任。

例如，很多人在判断自己访问的网站是否安全的时候，只是简单地看网站是否被加密，误以为，只要是被加密的网站，就是安全的，然而事实远非如此。加密网站所用的证书是一种很特殊的东西，它可以自己给自己颁发，但默认情况下不会被 Windows 或其他操作系统以及软件所信任。

因此，很多恶意软件的制作者就利用这种方式，自己给自己颁发一个证书，用证书加密伪装成银行的网站，然后用各种方法诱骗银行用户访问，并输入自己的账户信息。在老版本 Internet Explorer 中，这种问题并没有直接的提示，我们通过查看网站加密所用的证书虽然也可以看出端倪，但很多人根本没有意识到这个问题。

为了避免这种问题，在 Internet Explorer 8 中，如果某个网站加密所用的证书是自己给自己颁发的，不被 Windows 信任，那么 Internet Explorer 并不会直接显示该网站的内容，而是显示图 9-37 所示的警告信息提醒我们注意。只有单击“继续浏览此网站”链接才可以看到网站的内容。

图 9-38　网站使用了自己给自己颁发的证书

事实是否如此？让我们单击该链接，打开网站内容，然后看看网站所用的证书信息。单击该链接后，Internet Explorer 的地址栏会变为红色，同时在右侧会显示一个“证书错误”按钮，单击该按钮，并单击“查看证书”链接后，可以看到图 9-38 所示的“证书”对话框。

注意，图 9-38 中的“颁发给”和“颁发者”这两个地方显示的都是同一个人、公司或站点（为了保护隐私，真实的内容被涂掉了），或者有些情况下可能不会显示“颁发者”信息，就表示这个证书是自己给自己颁发的，不被根证书颁发机构所信任，当然也就不会被 Windows 信任。

然而对于使用这种证书的网站，还是要区别对待。

依然用上面的例子，假设是恶意网站的作者希望让我们以为这是银行网站，但我们遇到了这样的错误信息，这个网站肯定是有问题的。因为虽然购买受信任的证书需要花钱，但银行肯定不会缺这点钱。基本上所有正规的商业机构如果希望对网站进行加密（主要目的是防止窃听和证明自己的真实身份），肯定会使用被信任的商业证书，而不是这种自己给自己颁发的证书。

但也有这样的情况：有些非营利性的机构有自己的网站，同时希望对网站进行加密。这样做的主要目的只是防范网页服务器和浏览器之间的通信被窃听，而并不是为了证明自己的真实身份。这种情况下，为了节约成本，网站往往会使用自己颁发给自己的证书。因为为了实现加密的要求，这种免费获得的证书就足够了，没必要花钱购买。但 Internet Explorer 同样会认为这样的使用存在安全隐患，提醒我们注意。因此，只要认清这一点，就可以放心浏览这些网页了。

2．域名不同导致的证书错误

有时候访问一些商业性质的加密站点时也可能会遇到证书错误。这时很多人可能认为自己访问了钓鱼网站，或者自己的系统有问题。仔细检查就会发现，结果往往可能是虚惊一场。

例如，打开一个报告错误的加密网站，并查看证书的详细信息后，可以看到图 9-39 所示的界面。

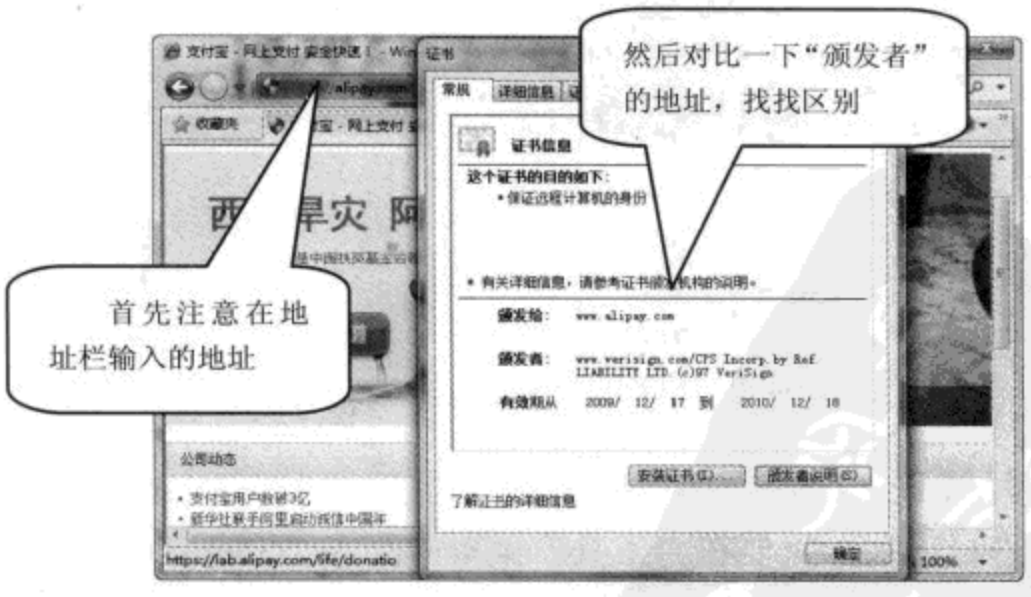


图 9-39　因为访问域名不同导致的证书错误

请留意浏览器地址栏显示的地址，是“alipay.com”，而证书显示的颁发给的地址是“www.alipay.com”，这才是造成此类证书错误的罪魁祸首。因为在 Internet Explorer 看来，“alipay.com”和“www.alipay.com”是两个截然不同的地址，虽然它们实际上可能是同一家公司同样内容的页面，但对于 Internet Explorer 来说，它们就是不同的，因此，才会报告证书错误。解决这类问题的办法也很简单，使用完整的地址访问网站即可。

9.1.2.2 仿冒网站筛选

在上文中已经介绍过什么是仿冒网站，同时也提到过怎样启用或者禁用 Internet Explorer 的 SmartScreen 筛选器功能。那么该功能具体是如何设置的？

当我们第一次运行 Internet Explorer 的时候，Internet Explorer 会打开一个设置页面，在这里可以对 Internet Explorer 的一些选项进行设置，其中包括 SmartScreen 筛选器功能的启用。如果当时没有启用该功能，或者希望修改设置，那么随时都可以按照下列方法进行：

STEP 01 在 Internet Explorer 的工具栏中单击“安全”按钮，指向“SmartScreen 筛选器”，随后即可通过“打开 SmartScreen 筛选器”以及“关闭 SmartScreen 筛选器”选项打开或关闭这个功能。

STEP 02 在打开该功能后，我们访问的每个网站地址都会被 Internet Explorer 提交到微软维护的一个在仿冒网站线数据库中进行查询。如果找到符合的记录，就表明我们访问的是一个仿冒网站，Internet Explorer 会停止显示网页，并给出提示。

STEP 03 如果不希望检查自己访问的每个地址，则可以关闭 SmartScreen 筛选器，但在访问到怀疑可能有问题的网站后，单击“安全-SmartScreen 筛选器-检查此网站”，仅对当前访问的网站进行检查。

STEP 04 如果检查结果正常，那么 Internet Explorer 将不对浏览进行干预，同时显示一个对话框告诉我们检查结果（如图 9-40 所示）；如果检查发现这是一个仿冒网站，Internet Explorer 会立刻显示警告信息。

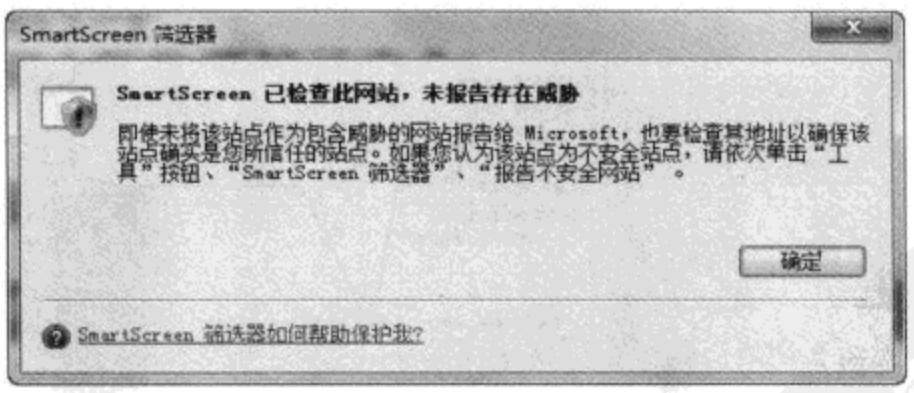


图 9-40 检查确认安全后的报告

STEP 05 如果访问的某个网站可能是仿冒网站，而 Internet Explorer 经过检查没有识别出来，这时候还可以进行上报。只要在“工具”菜单中指向“SmartScreen 筛选器”，接着单击“报告不安全网站”，Internet Explorer 就会自动打开报告页面，我们需要在页面上输入

必要的信息，然后提交即可。

Internet Explorer 的 SmartScreen 筛选器功能的正常工作取决于用户的积极报告。因为微软不可能将整个互联网上所有的仿冒网站都识别出来，因此，如果每个人都能积极报告，微软就会对报告中出现比较多的站点进行检查，一旦发现是仿冒网站，那么相应的信息就会被添加到在线数据库中，使得所有的 Internet Explorer 用户都能从中受益。

9.2　安全收发电子邮件

在互联网上，人们进行最多的应用，除了浏览信息外，可能就是收发电子邮件。正因为如此，很多怀有不同目的的人开始将电子邮件作为入侵操作系统或者实现其他不法目的的重要途径。

在 Windows 系统下，曾有两个电子邮件客户端软件在安全性问题上曾经广受争议，那就是微软的 Outlook Express（简称 OE）和 Microsoft Office Outlook（简称 Outlook）。对于这两个软件的安全性问题，主要表现在以下方面：

- 如果收到了 HTML 格式的邮件，这两个软件将会借助 Internet Explorer 的内核对邮件内容进行渲染（将 HTML 邮件中的 HTML 源代码转换为更加美观的邮件页面），因此，Internet Explorer 在安全性上的漏洞也将直接危害到 OE 和 Outlook。
- 对于 HTML 格式的邮件，这两个软件默认都是直接以 HTML 的形式查看，而非转换为纯文本查看，因此，邮件中一旦嵌入了恶意代码，将直接危害到整个系统。
- 这两个软件在垃圾邮件过滤方面的功能少得可怜。

发展到现在，对于新版本的 OE 和 Outlook，上述问题已经不再是问题了，因为：

- 对于 HTML 邮件，虽然 OE 和 Outlook 依然使用 Internet Explorer 的内核进行渲染，但在渲染的同时也会受到 Internet Explorer 中安全设置的限制。因此，在默认设置下，邮件中的恶意内容很难起作用。
- 可以通过设置选项让这两个软件将所有的 HTML 邮件转换为纯文本形式显示，这样就算邮件中包含恶意代码，也完全不会生效。而对于我们确认安全的邮件，还可以用很简单的方式重新转换为 HTML 格式查看。
- 新版本的 OE 和 Outlook 在反垃圾邮件、反钓鱼邮件方面新增的功能可以收到很好的效果。

很多人经常把 OE 和 Outlook 混为一谈，其实这两个软件还是有本质区别的。OE 是 Internet Explorer 中捆绑的一个电子邮件客户端软件，任何 Windows 用户都可以免费下载、安装和使用，这个软件适合一般用户，主要功能就是收发电子邮件和浏览新闻组。而 Outlook 是微软的 Microsoft Office 办公软件中的一个组件，收发电子邮件只是它最基本的功能，除此之外，Outlook 还可以用于管理日程、管理联系人和 Exchange 服务器联合使用。OE 更适合家庭用户和要求很简单的办公用户，而 Outlook 更加适合在企业网络中部署了 Exchange

的企业用户。

在 Windows 7 中的情况还有所变化。Windows 7 默认并未包含任何电子邮件客户端软件，但微软的 Windows Live 套件中提供的 Windows Live Mail 完全可以看做是 OE 的替代品。该软件需要单独安装（http://get.live.com）。

9.2.1 安全使用电子邮件的一些注意事项

目前广泛使用的电子邮件客户端软件有很多，限于篇幅，本书不可能面面俱到。下面首先介绍在使用电子邮件时最常见的安全和隐私问题，然后介绍防范这些问题的通用做法。

注意，现在绝大部分人通过两种方式收发电子邮件：使用网页浏览器进入邮箱的 Web 页面在线收发，或者通过客户端软件将邮件收取到本地进行收发。本节内容主要关注的是通过客户端软件收发的情况，如果主要是通过 Web 页面在线收发的，其实这等同于在浏览网页，因此，安全问题请参考 9.1 节的相关内容。

在使用电子邮件的时候，我们最常遇到下列问题：

- **垃圾邮件** 所有未经请求就主动发送的，不提供退订方法的，内容是我们不需要的邮件都可以看做是垃圾邮件。
- **染毒邮件** 邮件带有附件，附件文件可能感染了病毒，或者本身就是病毒，或者邮件是 HTML 格式，在 HTML 源代码中嵌入了恶意代码。
- **钓鱼邮件** 通过社会工程学原理诱骗我们访问某些网站，并输入自己的个人信息。

上述问题，只要采取一些很简单的措施，就能有效地避免被打扰，但前提是必须对这些邮件的基本原理有所了解。

9.2.1.1 垃圾邮件

发送垃圾邮件的人的动机很简单，无非就是希望我们能看到一些对他有利可图的东西，例如邮件内容是广告，或者宣传自己的观点。因为对于目前的大部分电子邮件系统，任何人只要知道我们的电子邮件地址，都可以给我们发送垃圾邮件。因此，要防范垃圾邮件，首先就要从源头着手，让朋友知道我们邮件地址的同时，避免让垃圾邮件发送者知道邮件地址。

1. 从源头杜绝

我们都知道，电子邮件地址的格式是“name@site.com”，因此，很多垃圾邮件发送者都编写专用的程序，自动在互联网的所有网页中搜索，如果找到符合上述格式的文字内容，就会记录下来。所以，如果我们需要在一些在线的论坛或者网页上留下自己的电子邮件地址，最好能采取一些措施。例如将符号“@”更换为“#”，这样邮件地址就变成了“name#site.com”，对于某些智能程度比较低的搜索程序，将不把这串文字看做是电子邮件地址。

因为使用这种方法的人太多，很多垃圾邮件发送者也开始改良自己的程序，如果遇到

类似“name#site.com”的字符，会将其中的“#”当做“@”记录下来，因此，这种方法目前不太可靠。

不过还有更简便的方法，因为电子邮件地址中的“@”符号读作“at”，而邮件地址中的“.”读作“dot”，因此，在需要留下自己邮件地址的时候，完全可以使用“nameATsiteDOTcom”的形式，甚至还可以在“AT”和“DOT”之间添加多个字符或者空格，目前很少有邮件地址收集软件能够识别这样的地址。

虽然这种方法对于英语为母语的人很方便，但对于讲中文的人就不那么方便了，很多人还不知道这样的“地址”是什么意思。因此，我们还可以考虑将自己的电子邮件地址转换为图片，然后将图片贴在需要留下邮件地址的地方。有很多在线网站可以帮我们制作这样的图片，例如 http://tinyurl.com/ybhw8hy，访问该站点后，在相应的文本框里输入自己的电子邮件地址，然后根据需要选择需要使用的字体、字号和颜色（如图 9-41 所示），随后单击“create image”，刷新后的页面上就会用图片的形式将邮件地址显示出来。我们可以将这个图片保存在自己的硬盘中，或者上传到可以引用图片的网络相册中，这样一旦需要在论坛或者网页上留下自己的邮件地址的时候，只要将这个图片上传，或者引用已经上传好的图片。对于访问网页，并且需要用电子邮件联系我们的人来说，完全可以在看到代表邮件地址图片后直接进行输入，但是对于在网络上自动搜索邮件地址的程序，它看到的只是一个图形文件，并且会跳过这个文件。

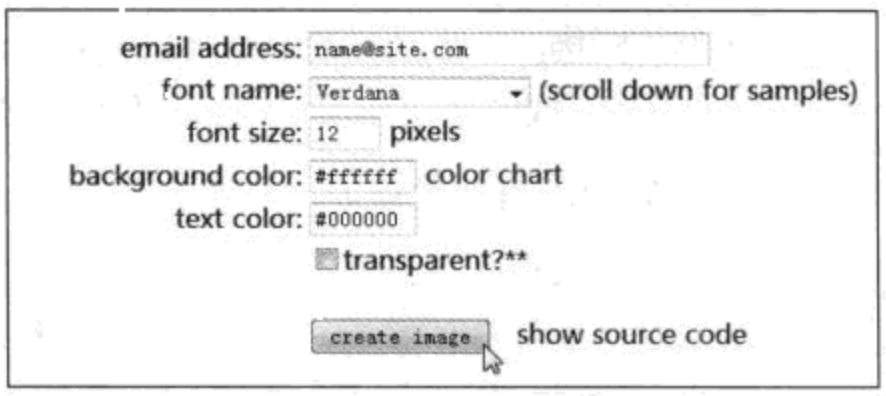


图 9-41　在此可将电子邮件地址转换为图片

通过这样的方法，只要电子邮件地址不被垃圾邮件发送者收集到，就能杜绝很大一部分垃圾邮件。

2. 使用软件的垃圾邮件过滤功能

虽然可以通过各种方法让自动收集邮件地址的程序看不到我们的地址，可垃圾邮件发送者也有新的办法。可能因为制造和传播垃圾邮件确实比较暴利，很多垃圾邮件发送者甚至开始雇人，用人工的方法查看大量网页，并从中找出有效的电子邮件地址，然后添加到自己的发送列表中。

另外，很多人甚至使用专用的软件对某个服务器进行群发，例如，假设垃圾邮件发送者希望所有的 Gmail 用户都收到自己的垃圾邮件，那么就会用软件对所有可能的地址（其

实就是利用各种数字和字母进行排列组合生成一系列用户名）进行发送。虽然这样听起来效率很低，可现在宽带网络的普及，以及高性能计算机的降价使得一些垃圾邮件发送者在一两个小时内就可以发送出去上百万封垃圾邮件，因而，大量发送邮件并不会产生太大的成本。

所以，除了保护好自己的邮件地址外，还可以使用电子邮件软件的垃圾邮件过滤功能，现在几乎所有新版本的电子邮件客户端软件都有这样的功能，我们会在下文进行介绍。

3．收到垃圾邮件后怎么办

前面已经说过，很多垃圾邮件发送者会利用群发软件向大量随机生成的地址发送垃圾邮件，而他并不知道哪些地址是有效，并且正在被使用的。我们一旦回复了这样的垃圾邮件，就表示在向垃圾邮件发送者大喊：我在这里，快给我发来更多垃圾邮件吧！

一旦回复了通过群发方式发来的垃圾邮件，那么发送者就会知道这个地址是真实存在的，并且还没有弃用。这样对方可能会将我们的地址添加到自己的“VIP 列表”中，以后每封垃圾邮件都会光顾我们的邮箱，同时他可能还会将自己的“VIP 列表”出售给其他垃圾邮件发送者，用不了多久，我们可能还会收到他的所有“业务伙伴”发来的更多的垃圾邮件。

另外，有些垃圾邮件中可能还冠冕堂皇地写着类似“抱歉打扰，如果您不希望收到我们的邮件，请点击这个链接退订”的话。这样的链接千万不要点击，这也是一种确认地址是否有效的方法，一旦单击其中的链接，产生的结果和直接回复垃圾邮件没什么区别。

收到垃圾邮件后，直接将其删除，或者拖放到电子邮件软件的垃圾邮件文件夹中即可。

4．防范通过其他方式进行的地址有效性确认

看过上面的内容后，很多人可能觉得，只要不回复垃圾邮件，也不点击垃圾邮件中的任何链接，对方就无法确认自己的地址是否有效了，其实还有更隐蔽的方法在等着我们。

假设邮件地址是“name@site.com”，收到了一封 HTML 格式的随机批量发送的垃圾邮件，发件人为了确认地址是否有效，在邮件中插入了一张 0×0 像素的图片（也就是说，这是一个虽然存在，但不会被觉察的图片），这个图片的地址结合了的收件人的邮件地址，例如可能是“http://www.spam.com/nameATsiteDOTcom.gif（这是一个虚构的地址，其中 www.spam.com 是垃圾邮件发送者管理的一台 Web 服务器）”这样的格式。当我们使用电子邮件预览或者打开这封邮件的时候，如果是直接查看 HTML 内容，邮件软件会从上述地址下载这张图片，垃圾邮件发送者就会记录这张图片的下载情况。也就是说，如果电子邮件软件下载了这张图片，就表示 name@site.com 这个邮箱是有效的，并且没有被弃用（毕竟无效邮箱或者被弃用的邮箱不会收到这封邮件，至少邮件中包含的这张图片不会被下载）。

为了防范通过这种方式确认地址的有效性，可以设置以纯文本方式查看所有的邮件，而只有在需要的时候才转换为 HTML 格式查看。或者有些软件也具备在以 HTML 格式查看邮件的同时不下载任何外部图片。只要邮件中的图片不被下载，发件人自然无法确认地

址是否有效。

5. 注意邮件回执功能

邮件回执功能可以理解为邮件的收条。例如，当我们给别人发送邮件时，可能很想知道对方有没有收到或打开这封邮件，这时候就可以请求邮件回执。这样当对方收到我们的邮件后，取决于对方电子邮件软件的设置，软件可能会询问收件人，是否发送邮件回执。通常在这个询问对话框中还会有类似“以后不再询问”的选项，如果选中该选项，那么这个人以后收到所有请求回执的邮件后，软件都不再询问，直接自动发送回执。

很多垃圾邮件发送者已经开始利用这个功能，例如，给他们发出的所有垃圾邮件都设置了请求回执的操作，收件人收到这样的邮件后，如果设置了自己的软件自动发送回执，那么将会向垃圾邮件发送者发送一封回执，对方可以通过收到的回执判断邮箱地址的有效性。

因此，请一定要慎用邮件回执功能，至少不要启用自动发送回执的功能。

9.2.1.2　防范染毒邮件

电子邮件中的病毒主要以两种形式存在：给 HTML 格式的邮件源文件中嵌入恶意代码，或者在邮件中附加带有病毒的文件。一旦查看或预览这样的邮件，或者打开了邮件的附件，病毒就可能感染系统。

为了预防邮件中的病毒，可以首先确保 Internet Explorer 的默认安全设置，因为上面已经说过，很多电子邮件软件都是借助 Internet Explorer 的核心来渲染 HTML 邮件的，因此，邮件的显示会受到 Internet Explorer 安全功能的限制。

另外，可以安装反病毒软件，因为几乎所有主流的反病毒软件都带有电子邮件监控功能，会在收到邮件的时候扫描邮件中的内容，一旦发现邮件中带有病毒（无论是恶意代码还是染毒附件），都会提醒我们注意，并可以删除或者隔离这样的邮件。

为了预防电子邮件附件中的病毒，在打开电子邮件附件的时候一定要谨慎，即使邮件来自熟悉的人，也不能大意。因为对方可能无意间中毒了，病毒会自动搜索当前用户的联系人，并给每个联系人发送带有病毒的邮件。因此，收到的来自熟人的邮件可能并不是他本人发送的。

除此之外，Windows 对于文件扩展名的处理也可能导致我们无意中打开染毒文件。在 Windows 中，默认情况下会隐藏已知文件类型的扩展名，例如，对于一个名为“flower.jpg”的文件，因为 Windows 可以直接打开.jpg 格式的图形文件，这属于已知的文件类型，因此，在 Windows 资源管理器中，Windows 会将该文件显示为“flower”。那么什么又是未知文件类型？假设系统中没有安装 Adobe Reader 或者其他任何可以打开 PDF 文件的软件，那么一个名为“file.pdf”的文件在我们的系统中就会显示为“file.pdf”，而不会显示为“file”。

假设有一个名为“flower.jpg.exe”的文件（.jpg 是主文件名的一部分，只有.exe 才是扩展名），这实际上是一个可执行文件，但因为 Windows 默认不会显示已知文件类型的扩展

名，因此，这个文件在 Windows 中会被显示为“flower.jpg”。如果收到包含这种附件的邮件，那么在电子邮件软件中，这个文件的名称就会被显示为“flower.jpg”。如果不够仔细，有人可能会觉得这是一个图形文件，不会对系统产生危害，我可以放心打开。于是双击了这个文件，但图片内容怎么没有显示出来？硬盘为什么会狂转？怎么死机了？

为了防范这种问题，可以按照下列方法设置让 Windows 显示已知文件类型的扩展名：

STEP 01 打开“计算机”窗口，按下键盘上的“Alt”键以显示菜单栏。

STEP 02 在菜单栏上依次单击“工具”→“文件夹选项”，打开“文件夹选项“对话框。

STEP 03 打开“查看”选项卡。

STEP 04 在“高级设置”选项下，取消对“隐藏已知文件类型的扩展名”选项的选择。

9.2.1.3 防范钓鱼邮件

网络钓鱼是近年来新发展起来的一种网络诈骗方式，这种方法的技术含量并不高，但是很容易得手。

网络钓鱼的形式虽然多种多样，但是基本原理和预防方法都是一致的。关于这种诈骗的详细信息，请参考 9.2.2.3 节的内容，在那里会专门针对各种钓鱼方式进行介绍。

9.2.2 Windows Live Mail 中的邮件安全特性

本节要介绍在 Windows Live Mail（下文统一简称为 WLM）中如何更安全地收发电子邮件。WLM 是一个免费软件，可以安装在 Windows Vista/7 等系统中，我们可从 http://get.live.com 网站下载并安装。

为了不断地加强自家多款电子邮件软件的反垃圾邮件能力，微软会不定期地提供新版的垃圾邮件筛选器，只有及时安装这些筛选器，才能尽可能多地过滤不安全邮件。因此，请定期使用 Microsoft Update 网站进行更新。

9.2.2.1 防范垃圾邮件

在 WLM 中，默认就已经启用了垃圾邮件过滤功能。WLM 会对收到的每封邮件进行判断，如果觉得是垃圾邮件，就会将其放入“垃圾邮件”文件夹中；如果判断是正常邮件，才会将其放入“收件箱”。不过默认设置的 WLM 在判断垃圾邮件方面可能无法很好地满足我们的需要，我们可以根据实际情况对其进行设置，方法如下：

STEP 01 在 WLM 的主界面上按下“Alt”键以显示菜单栏，接着在菜单栏中依次单击“工具”→“安全选项”，打开“安全选项”对话框。有关垃圾邮件的设置，需要在该对话框的“选项”、“安全发件人”、“阻止发件人”，以及“国际”这 4 个选项卡下进行。

STEP 02 在“选项”选项卡下可以设置的内容如图 9-42 所示。

首先可以根据实际需要设置垃圾邮件保护级别，通常，越高的级别，越可以保证识别出隐蔽的垃圾邮件，但有可能将原本正常的邮件（例如，朋友和我们讨论某个新上市的产品，但 WLM 觉得这是垃圾邮件发送者在向我们做广告）判断为垃圾邮件。一般情况下可

以选择“高”这个保护级别，这样大部分垃圾邮件都将被识别出来。

如果只是需要和少数的几个人通过电子邮件进行交流，可以在将这些人都添加到安全发件人列表（具体做法请参考下文）后，在这里选择“仅安全列表”，这样只有发件人地址符合安全列表中的描述后才会被判断为正常邮件，其他邮件都会被判断为垃圾邮件。

如果选中“永久删除可疑的垃圾邮件”选项，那么一旦 WLM 判断某封邮件是垃圾邮件，将会直接将其删除，而不是放入“垃圾邮件”文件夹。一般不建议选择该选项，因为 WLM 的判断功能可能会有些小的失误，如果正常邮件被判断为垃圾邮件，而选择了该选项，正常邮件也会被直接删除。

和 Internet Explorer 中的仿冒网站筛选功能类似，WLM 的垃圾邮件判断功能也是需要不断学习才能提高的。毕竟垃圾邮件发送者发送垃圾邮件的技术在与时俱进，那么反垃圾邮件技术也不能松懈。在选中“向 Microsoft 及其合作伙伴报告垃圾邮件”选项后，如果我们将 WLM 识别为正常邮件的邮件重新标注为“垃圾邮件”，那么 WLM 将自动把这封邮件的特征匿名发送给微软，微软可以根据我们的反馈研究新出现的垃圾邮件的特点，并更新 WLM 的垃圾邮件过滤机制。当然，为了保护隐私，正常邮件的内容是不会被发送出去的，只有被 WLM 判断为正常，且将其重新标注为垃圾邮件的内容才会被发送。

STEP 03 在“安全发件人”选项卡下，可以设置的内容如图 9-43 所示。

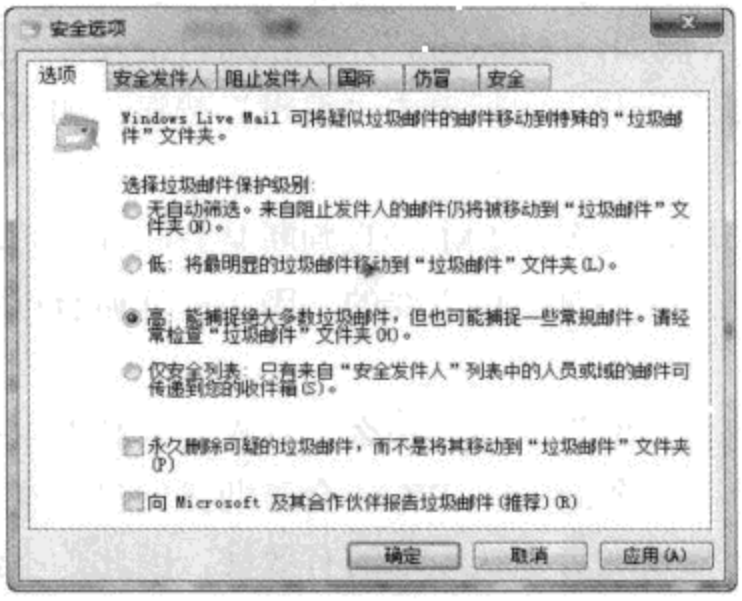


图 9-42　有关电子邮件的常规安全选项

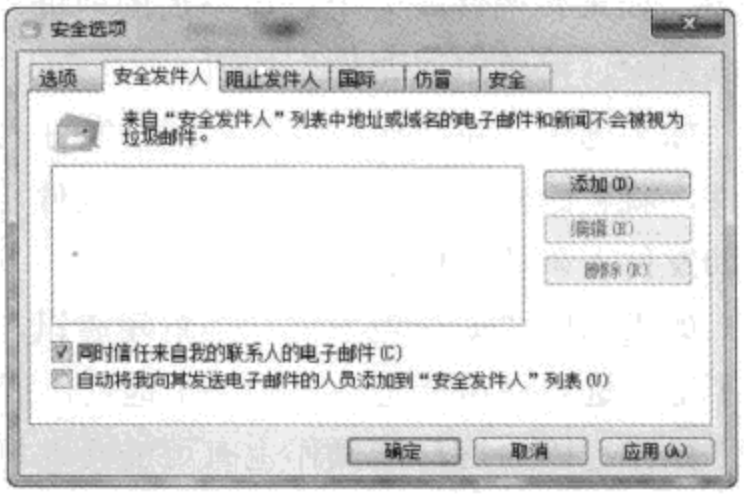


图 9-43　管理安全发件人

所谓“安全发件人”，是指只要是来自这些地址的邮件，无论内容如何，都会被 WLM 判断为正常邮件，不会被放入垃圾邮件文件夹。因此，可以通过“添加”按钮将某个具体的地址（例如“name@site.com”）或者某个域（例如“site.com”）添加到安全发件人列表中。如果希望修改一个已经添加的地址，可以在将其选中后单击“编辑”按钮，单击“删除”按钮可以将其删除。

如果选中“同时信任来自我的联系人的电子邮件”选项，那么对于已经保存在 WLM 联系人程序中的联系人，无论他们的邮件地址有没有添加到安全发件人列表中，都会被 WLM 认为是安全的。

如果选中“自动将我向其发送电子邮件的人员添加到‘安全发件人’列表”选项，那么，无论我们是主动回复了一封陌生人的邮件，还是给陌生人发送了一封邮件，对方的地址都会被添加到安全发件人列表。

STEP 04 在“阻止发件人”选项卡下，可以设置的内容如图 9-44 所示。

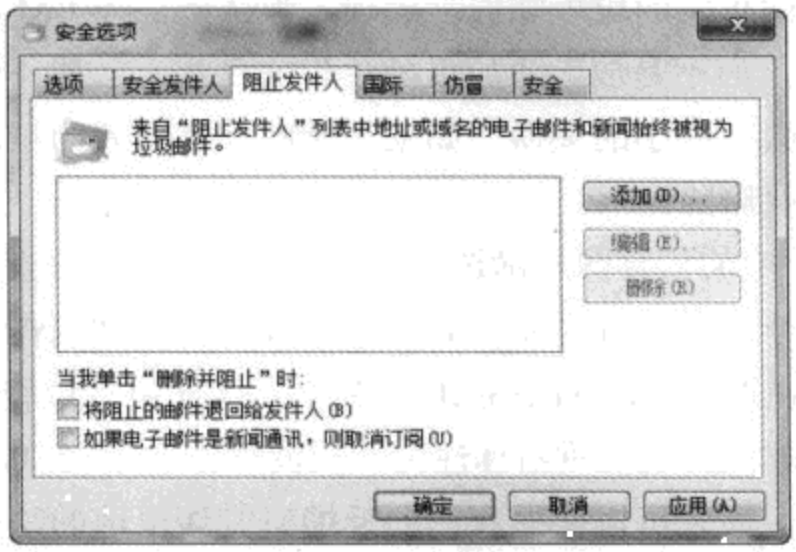


图 9-44　管理被阻止的发件人

所谓“阻止发件人”，是指对方无论发来什么内容的邮件，都会被 WLM 判断为垃圾邮件，并放入到“垃圾邮件”文件夹或直接删除。同样，可以通过“添加”按钮将某个具体的地址（例如，“name@site.com”）或者某个域（例如，“site.com”）添加到阻止发件人列表中。如果希望修改一个已经添加的地址，可以在将其选中后单击“编辑”按钮；如果要将其删除，可单击“删除”按钮。

如果选中“将阻止的邮件退回给发件人”选项，那么 WLM 一旦判断某封邮件为垃圾邮件，就会给对方发送一封邮件通知这件事，这显然不是我们需要的，因为这样做有可能帮助发件人确认我们的地址有效。

如果选中“如果电子邮件是新闻通讯，则取消订阅”选项，那么一旦收到的邮件中提供了退订选项（可能是回复到某个地址，或者单击某个链接），WLM 会帮助我们自动执行退订操作。因为这样的操作也有可能帮助垃圾邮件发送者确认地址的有效性，因此，不建议选择。

STEP 05 在“国际”选项卡下，可以针对不同的语言或者编码方式来判断什么样的邮件是垃圾邮件。打开“国际”选项卡，单击“阻止的顶级域列表”按钮后，可以看到图 9-45 所示的对话框。

不同国家和地区都有对应的顶级域名，例如，中国大陆的顶级域名是“CN”，中国香港特区的顶级域名是“HK”，因此，可以通过顶级域名来判断垃圾邮件。原理是：假设从来不需要和安道尔人有任何联系，但某天收到了一封顶级域为安道尔的地址发来的邮件，很显然，八成是垃圾邮件。因此，通过这个功能，可以选中某些国家或地区的顶级域，这样来自该域的邮件将直接被判断为垃圾邮件。注意，该功能对于没有使用国家和地区顶级

域名的地址（例如，site.com）无效。

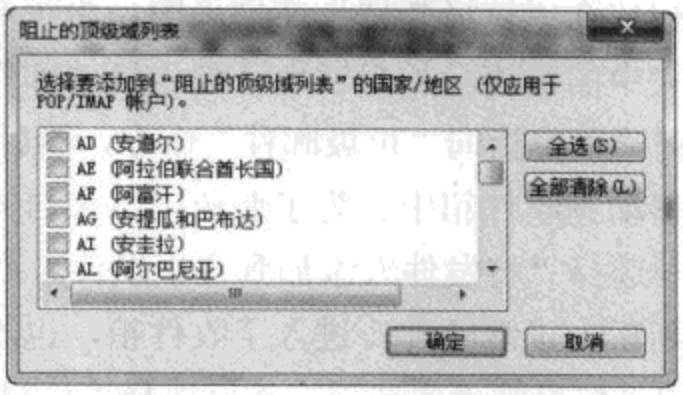


图 9-45　通过发件人地址的顶级域阻止

STEP 06 除了可以通过邮件地址的顶级域名来判断垃圾邮件外，还可以通过邮件正文所用的编码方式来判断。例如，对于使用简体中文的用户，一般邮件的编码方式可能是“GB2312”或者“UTF8”；而使用繁体中文的用户，一般邮件的编码方式可能是“BIG5”或者“UTF8”。如果不懂日语，也没有跟使用日语的人有任何联系，但却收到了日语编码的邮件，那么经过设置，WLM 就可以将这类邮件判断为垃圾邮件。

在“国际”选项卡下单击“阻止的编码列表”按钮，随后可以看到图 9-46 所示的对话框。只要在这里选中所有不会使用的语言，WLM 就会在收到相应语言编码的邮件后自动将其判断为垃圾邮件。

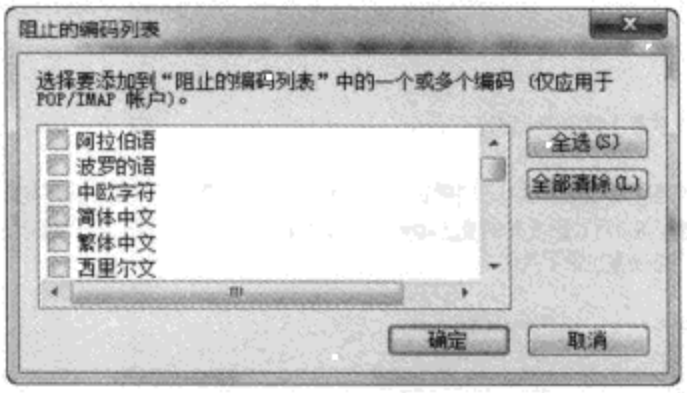


图 9-46　通过邮件的编码方式识别垃圾邮件

WLM 本身具有自动发送邮件回执的功能，因此，如果希望对该功能进行配置，请这样操作：

STEP 01 在 WLM 的主界面上按下“Alt”键以显示菜单栏，然后依次单击“工具”→“选项”，打开“选项”对话框。

STEP 02 打开“回执”选项卡。

STEP 03 在“返回已读回执”选项下，请确保选择了“从不发送已读回执”或者“对于每个已读回执请求都通知我”两个选项。

有关 WLM 在垃圾邮件方面的设置就是这些。那么在使用过程中还需要注意什么问题？

首先需要注意一点，那就是经常查看“垃圾邮件”文件夹中的内容。因为 WLM 是根

据一些自动的算法来判断一封邮件是不是垃圾邮件的，而有时候，这种方式可能会造成误判，导致原本正常的邮件被放在“垃圾邮件”文件夹中。为了避免误事，请每隔一段时间就查看一下垃圾邮件文件夹中的内容。如果发现了被误判的邮件，只要用鼠标右键单击列表中的目标邮件，并在右键菜单中指向“垃圾邮件”命令，然后选择“标记为非垃圾邮件”选项，即可将该邮件重新移动到收件箱中。为了避免以后来自同一个发件人的邮件再次被误判，还可以从右键菜单中选择“将发件人添加到安全发件人列表”命令。

如果一封垃圾邮件被判断为正常邮件，进入了收件箱，也不用担心，因为可以在目标邮件上单击鼠标右键，指向“垃圾邮件”选项，然后选择“标记为垃圾邮件”，或者直接单击 WLM 工具栏上的“垃圾邮件”按钮。

对于包含了外部图片的 HTML 邮件，默认情况下，虽然 WLM 会显示 HTML 形式的邮件，不过并不会下载外部图片（除非发件人是我们的联系人，或者发件人的地址位于安全发件人列表中）。当打开这样的邮件后，可以看到图 9-47 所示的界面。

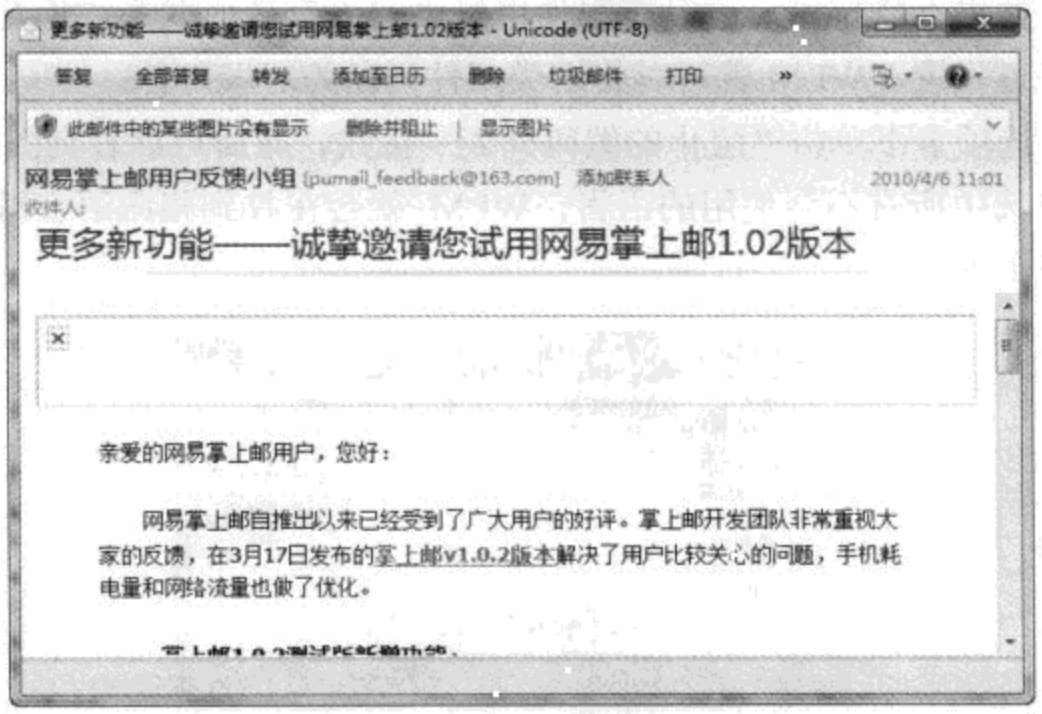


图 9-47　邮件中被阻挡的外部图片

首先注意，在邮件窗口的工具栏底部出现了一个黄色的信息栏，就像 Internet Explorer 中的信息栏那样，提醒我们有一些图片没有显示出来。同时在邮件正文中，原本应该显示外部图片的地方只出现了红叉。如果觉得这封邮件是安全的，可以单击信息栏上的“显示图片”链接查看邮件中的图片；如果希望以后来自同一个发件人的邮件自动显示所有的外部图片，也可以单击“添加联系人”链接，将发件人添加到联系人中，这样以后对方发来的邮件中无论是外部的图片还是内部的图片，都会被自动显示。

另外有一点需要注意，有人可能会发现，为什么有时候陌生人来的垃圾邮件里的图片有些显示出来了，有些没有显示，难道这个功能也会失效？其实这个功能只针对外部图片，也就是说，没有包含在邮件内容中的需要在互联网上下载的图片。对于包含在邮件内部的图片，不会受到该功能的影响。

9.2.2.2　防范染毒邮件

在上文中已经介绍过，病毒通过电子邮件传播主要有两种途径：以恶意代码的形式嵌入 HTML 邮件中；以染毒附件的形式附加在邮件上。因此，首先需要对 WLM 的安全选项进行一些设置，具体操作如下：

STEP 01 在 WLM 的主界面上按下“Alt”键以显示菜单栏，接着依次单击“工具”→“安全选项”，打开“安全”选项卡，随后可以看到图 9-48 所示的界面。

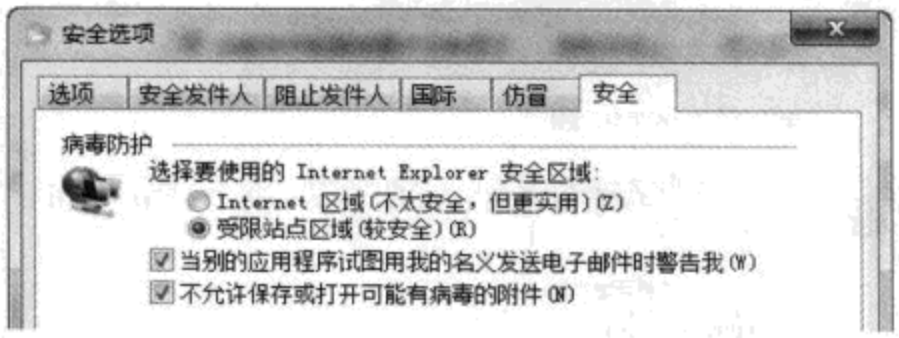


图 9-48　和反病毒有关的安全选项

STEP 02 在这里需要关注的是“病毒防护”选项下的内容。

- 在“选择要使用的 Internet Explorer 安全区域”下，建议选择“受限站点区域”。因为前面已经介绍过，WLM 在显示 HTML 格式的邮件时将使用 Internet Explorer 的内核进行渲染，因此，Internet Explorer 的安全设置就完全可以影响到 WLM 的安全性。通过在这里选择“受限站点区域”，WLM 会强制让收到的所有 HTML 邮件都受到 Internet Explorer 中受限站点区域的安全限制(可以说是 Internet Explorer 能够提供的最大程度的限制)。在这样的设置下，就算 HTML 电子邮件中嵌入了恶意代码，因为在受限站点区域下无法生效，根本不会危及系统安全。
- 在选中“当别的应用程序试图用我的名义发送电子邮件时警告我”选项后，如果系统中有其他程序试图借助 WLM 中添加的账户主动向外发送电子邮件（感染了某些通过电子邮件传播的蠕虫病毒后会有这样的现象），WLM 就会向我们询问，并提供允许和拒绝的选项。
- 如果选中“不允许保存或打开可能有病毒的附件”选项，当收到带有可执行文件（例如.exe、.com、.bat 等）作为附件的邮件后，WLM 将不提供保存附件或打开附件的选项，而被认为是安全的文件类型（例如.jpg、.png 等）才允许直接打开或保存。

STEP 03 依然是在 WLM 的主窗口中，按下“Alt”键以显示菜单栏，单击“工具”→“选项”，打开“选项”对话框，进入“阅读”选项卡，选中“以纯文本方式阅读所有邮件”选项，这样日后收到的 HTML 邮件都会以纯文本的方式显示。

基本上，WLM 中有关反病毒的设置选项就是这些，我们来看看成果吧。

在设置了用纯文本方式打开 HTML 邮件后，当我们打开一封 HTML 邮件，看到的将是图 9-49 所示的界面。请和图 9-47 进行比较，这是同一封 HTML 邮件在 HTML 视图下和

纯文本视图下的不同外观。从中可以看出，虽然转换为纯文本，但看到的并不是所有的HTML 源代码，而是从中挑选出来的邮件正文内容。因此，用纯文本形式查看电子邮件，损失的仅仅是邮件内容中美观的排版、图片以及文字样式，但是邮件本身的内容不会有任何丢失。

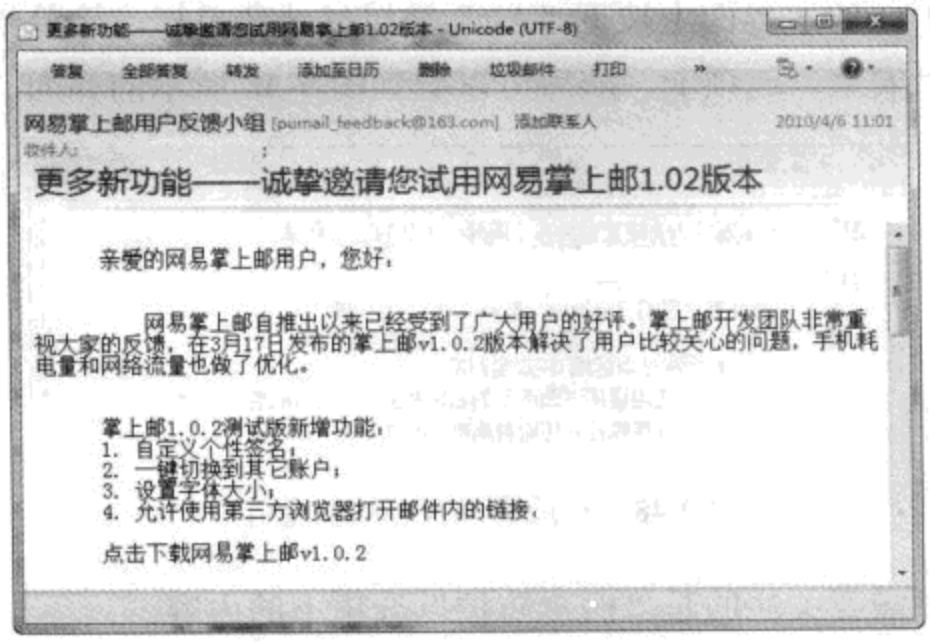


图 9-49　用纯文本格式查看 HTML 邮件

用纯文本形式查看 HTML 邮件，不仅速度更快，而且更安全，因此，推荐大家使用。在这样的方式下，如果确实需要看到邮件的 HTML 视图，也是很简单的，只要在图 9-49 所示的界面上单击“转发”按钮，邮件内容就会以 HTML 格式呈现在信邮件窗口中。只不过此时不需要真正发送这封邮件，看完后直接关闭邮件窗口即可。

对于以附件形式传播的病毒，如果收到了这样的邮件，在 WLM 中查看的时候，WLM 会用红色的信息栏提醒我们注意，并且禁止我们对这样的附件进行任何类型的操作。

这种情况并不意味着附件一定就是存在病毒的，只是说明因为附件是可执行文件，因此，存在安全隐患，所以，WLM 不允许打开或保存该文件。如果确定这个文件是正常的，并且希望打开，那么就必须联系发件人，让发件人重新发送，但在发送前，将这个附件进行压缩（压缩文件不被归类为“危险”文件）。或者也可以在图 9-48 所示的界面下取消对“不允许保存或打开可能有病毒的附件”选项的选择，但是要记住，为了确保安全，在使用完这个附件后，一定要重新选中该选项。

如果收到的附件是被 WLM 认可的“安全文件”，同样不能大意。因为 WLM 本身没有扫描病毒的能力，它并不知道哪个附件是感染病毒的，而只是通过文件的扩展名进行判断。因此，在需要打开一封邮件中被 WLM 判断为“安全文件”的附件时也要小心谨慎，尽量不要直接打开附件文件，而是将其保存到硬盘上一个顺手的位置，然后使用反病毒软件对文件进行扫描。只有确认文件中不包含病毒的情况下再打开。

9.2.2.3　防范钓鱼邮件

在 WLM 中，钓鱼邮件基本没有太多的选项可以设置，因此，只要直接使用该功能即可。

让我们假设一个很常见的钓鱼邮件类型：收到了一封发件人显示为“Paypal Security”的邮件（Paypal 是国外一个在线支付网站，类似国内的支付宝），发件人的地址是“Secure@paypal.com”。邮件的中心内容是说，因为某些原因，我们的账户被限制使用了，而我们必须使用自己的 Paypal 账户和密码登录“官方网站”，然后进行某种操作。最后，这封邮件还很体贴地提供了用于打开“解决中心”地址的链接，我们只要单击这个链接，就可以登录并进行操作。看看 WLM 会怎样对待这封邮件，如图 9-50 所示。

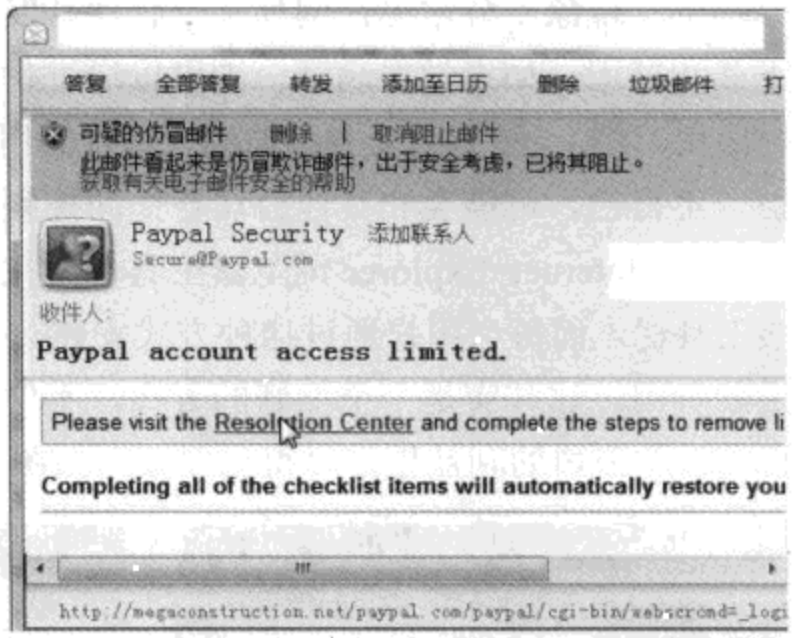


图 9-50　仿冒邮件会被用明显的方式标注出来

首先，在邮件窗口顶部再次出现了红色的信息栏，告诉我们这是一封可疑的仿冒邮件，在这种情况下只能查看邮件的内容，无法点击邮件中的任何链接。那么这种伎俩到底是如何被识破的？让我们将鼠标指针放在邮件上提供的用于登录 Paypal 的链接上，然后看看窗口底部状态栏中显示的地址。很明显，如果是需要登录 Paypal 的链接，那么这个链接应该是指向 Paypal 官方网站（www.paypal.com）的，但通过状态栏我们可以看出，这个链接实际上是指向一个“.net”站点，虽然无法直接单击链接打开该网站，不过可以相信该网站的页面设计肯定和 Paypal 官方网站一模一样。

说到底，这类钓鱼邮件的主要目的就是诱骗我们到一个冒充的某机构官方网站上提供自己的个人信息。因此，我们只要细心，完全可以自己识破其中的诡计，例如，在电子邮件中看到链接后，先不要急着点击，而是将鼠标指针放在链接上，看看 WLM 窗口底部状态栏中显示的链接实际指向的位置和自己要浏览的地方是否一致。这个过程中一定要细心，并对自己要浏览的网站地址很熟悉，如果粗心大意，看到“www.cnnbchina.com”就以为是招商银行的官方网站，结果肯定会吃亏。

当然，预防这类问题最简单的办法就是不要点击邮件中的链接。例如，邮件中不是说我们的 Paypal 账户被限制了，需要在网页上登录并进行一些设置吗？可以啊，虽然邮件中有直接打开登录页面的链接，但我们不点击它，相反直接打开一个浏览器窗口，输入要去的网站域名并登录，然后看是否真的需要进行邮件中提到的操作。

9.3 软件安装时的注意事项

除了通过网络进入到系统中外，病毒和恶意软件的另一个入侵途径是通过感染的文件，绝大部分计算机病毒都是通过这种方式传播的。因此，在保证自己的网络安全和上网安全之外，还要注意安装的软件或者打开的文件是否安全。

目前，软件行业的“捆绑”现象十分常见，例如某个软件开发公司开发了一个共享软件，放在互联网上供人下载和试用，如果觉得满意，则可以通过付费方式获得完整版（这属于共享软件领域的一种通用习惯）。然而因为各种原因，付费的用户很少，开发这个软件的公司自然无法获得收益，不得已，可能会和其他公司合作间接赢利，例如，很多公司开发的软件中都捆绑了 Google 的 Internet Explorer 浏览器工具栏，在安装这些软件的时候，用户可以选择是否安装该工具栏，而每当用户通过这种方式安装一个工具栏，Google 公司就会给这家软件公司一定的费用。这其实是一个很好的方式，不仅让我们可以更好地使用共享软件，而且开发共享软件的公司的利益也可以得到保证（如图 9-51 所示）。

图 9-51　只要注意捆绑软件提供的选项，就可有选择地安装程序

但是很明显，对于共享软件开发商来说，上述这种方式存在一个很大的不足：**用户具有选择权**！用户可以选择是否安装捆绑的软件，而只有安装了，软件公司才能获得收益。因此，为了能够获得最大的收益，很多软件公司开始采取一些狡猾的手段，例如捆绑其他公司的软件，也提供是否安装的选项，但默认是选中的，这也就意味着，如果安装软件的时候不够仔细，一路单击“下一步”按钮，可能会给系统中安装不需要的软件。更有一些无良的厂商，根本不告诉我们自己的软件中捆绑了其他软件，而且也不会询问是否安装，只要安装他们的软件，就会连捆绑的软件一起安装到系统中，这个过程完全是不会被用户察觉的。

可能有人觉得，这无非就是捆绑了一些软件，如果需要捆绑的软件，那自然很好，可

以直接使用，很方便；如果不喜欢捆绑的软件，那把它卸载掉不就好了？是，理论上，这样也可以。但问题在于，有些捆绑的软件为了达到悄悄潜伏在系统中不被用户察觉，或者防止用户卸载的目的，往往会借助一些病毒才会使用的“无赖”手法，一旦这类软件被安装到系统中，除非重新安装操作系统，否则就会在系统里扎根。

更严重的情况是，这些软件可能目的并不像宣称的那样单纯。例如，有些捆绑的软件会监视我们在 Internet Explorer 中浏览的网页记录，并定期将记录信息传出去；有些捆绑的软件会偷偷修改 Internet Explorer 甚至系统的某些设置（例如首页设置），将其锁定，不允许用户更改；有些会不定时地在系统中弹出广告。更有甚者，如果无意中安装了具有类似功能的多个被捆绑软件，这些捆绑的软件之间有可能会产生冲突，导致程序或者系统无法正常工作。

这类软件的安装很隐蔽，不容易被发觉，而且很难彻底清除，这些都是病毒才具有的特征。但又因为这类软件很少主动传播，或者破坏系统和数据，因此，这类软件往往有一个更形象的名称：灰色软件（有些人直接称呼其为“流氓软件”）。

其实对于捆绑灰色软件，问题还不是最严重，更严重的是直接捆绑病毒、木马程序或者蠕虫病毒。例如，假设某个专门提供软件下载服务的网站，因为软件种类多，下载速度快，很受大家欢迎，但这个网站的安全意识不够，导致网站服务器被黑客攻击，黑客给网站提供下载的所有文件中都捆绑了木马程序。这样当大家从该网站下载软件并安装时，如果没有安装反病毒软件，或者反病毒软件没有更新病毒定义，就有可能直接导致很严重的后果。影响系统正常运行倒是小事，大不了重新安装或者从备份中恢复，但如果损失了重要数据，甚至银行账号之类的信息，其代价就太大了。

怎样预防这类问题？下面将详细介绍。

9.3.1　从可信的来源下载软件

如果希望下载某个软件，首选的途径就是访问软件开发商的网站，从开发商网站中下载。因为这种情况下获得的软件是最可靠的，下载到的程序里面不会有被恶意捆绑的内容，除非软件开发商给自己的程序中捆绑了其他软件。

如果不知道自己需要的软件的开发商网站地址，或者因为其他原因想要从下载网站下载，那么至少请在口碑好的专业下载网站下载。但如果在一些不太知名的陌生的网站下载，往往就需要很小心了。

除了软件的下载途径外，软件的版本是否可信也是很重要的问题。例如，有很多出色的软件是外国人编写的，往往是英文或者其他外文界面，这对于不懂外文的人来说往往会造成很多使用上的困难。为了解决这种问题，网上有很多热心人会对软件进行“汉化”，也就是将原本的外文界面的软件在保证所有功能不受影响的前提下，将界面语言变为我们熟悉的中文。

汉化的方式有很多，例如，可能需要用下载的汉化文件替换外文的原始文件；或者将

汉化过的语言文件放在软件的安装目录下，然后从软件的设置界面中选择使用中文界面。因为汉化方式多种多样，这对于很多新手来说依然存在一定的困难。为了解决这些困难，体贴的汉化人往往还会提供汉化程序。例如，在安装了外文版的软件后，运行汉化程序，汉化程序就会自动采取需要的操作，将软件界面变为中文，或者也有可能直接提供汉化后的软件安装文件，这样安装好的软件就已经成了中文界面。然而这里面就隐藏了很多风险。

另外一点就是修改版的软件。一个软件的用户数量可能会有很多，然而大量的用户可能对同一个软件都会具有不同的要求，例如，有些人希望某软件在实现一个功能的时候这样做，而有些人希望某软件在实现同一个功能的时候那样做。软件开发公司不可能照顾到所有的用户，因此，修改版的软件应运而生了。

例如，Foobar 2000 是一个很出色的音频播放软件，该软件小巧、界面简洁、自定义功能强，很受大家欢迎。但也不是所有的人都对这个软件满意，例如，有些人希望这个软件能够支持更多的格式，有些人希望这个软件的界面更加美观，因此，熟练的用户可能会根据自己的实际需要给 Foobar 2000 安装能够实现更多功能的插件。然而并不是每个人都有这样的技术条件，更多的人更加习惯于使用别人修改过的版本。例如，网上盛传的 Foobar 2000 的各种美化或者增强功能的版本就有几十种之多，安装这些被别人修改过的版本后，Foobar 2000 的界面可以更漂亮，其功能也能更多，相当方便。

运营软件下载网站需要购买服务器、租用网络线路，耗资不菲；软件汉化人或者修改版软件制作人可能牺牲了自己的工作或休息时间，为大家提供更好用的软件。那么这些人的付出是否可以获得最直接的经济回报？这种情况很少发生。因此，少部分人开始采取一些不光彩的手段，和某个灰色软件开发公司达成协议，给每个文件都捆绑灰色软件，然后向这个灰色软件开发公司收费；你们都喜欢用我的汉化或者修改版软件？那好，我在软件里预置一个功能，收集大家的网页浏览习惯，然后统一发送给我，我再根据你的浏览习惯将你可能感兴趣的广告推送到你的桌面上，谁想通过我的汉化或者修改版软件做广告，就得付费。

虽然这类情况很少，但确实存在，而且造成的危害性非常大。为了防范这种危险，有如下建议：

- 如果要下载一个软件，首选通过软件开发商的官方网站下载，其次，推荐从口碑比较好的专业软件下载网站下载。请尽量不要从不知名的网站下载。
- 很多专业下载网站目前都提供了评价功能，可以供网友们对每个软件的“捆绑”情况进行评价和打分。如果常去的下载网站有这样的功能，最好在下载之前能够看看别人是怎样评价要下载的软件的。
- 如果发现自己下载的软件是外文版，在寻找汉化之前，请首先检查软件的设置，是否提供了多语言选项，其次访问开发商网站，看是否提供有官方的语言包或者汉化程序。如果通过官方的途径无法获得汉化，则可以从一些专业的或者口碑比较好的汉化网站下载汉化文件。

- 尽量不要使用修改版的软件，因为修改者的技术水平如果不过关，或者操作不够仔细，可能给原本正常的软件带来漏洞或其他故障。如果一定要用修改版的软件，请选择口碑比较好的版本。

9.3.2　安装时的注意事项

下载到需要的软件后，在双击开始安装之前，需要做一些准备工作。

首先应该知道，我们下载的这个软件在网上肯定还有其他人已经下载并安装和使用，因此，在安装之前可了解一下他们对这个软件的评价。例如，如果有人已经安装了这个软件，发现软件中偷偷捆绑了插件，或者导致其他问题，往往会在网络论坛或者 Blog 中提出。我们可以通过这些内容对软件的口碑有一个大致的印象。

打开浏览器，并进入到惯用的搜索引擎网站上，接着使用类似这样的格式输入关键字："软件名版本号"，随后按下回车键搜索即可。这里需要注意的是，对于"软件名"，建议输入得越详细越好。例如，如果安装了一个美化版 Foobar 2000，这个美化版的名字叫做"刘晖美化版 Foobar 2010"，那么只输入"Foobar"进行搜索，找到的结果中肯定会包含大量不需要的内容，因此，可以将美化/汉化/增强版本的作者名字、软件的名称，以及软件的版本号都输入进去。输入的关键字越详细，找到的内容就越准确。

如果经过搜索，发现打算安装的软件有不好的评论，建议一定要谨慎。这时候可以考虑其他类似功能的版本，例如对于大部分知名软件，汉化它的人肯定不止一个，既然这个人的汉化程序有问题，那么不妨试试看别人的汉化程序。

如果经过搜索发现打算安装的软件完全没问题，至少要装的软件目前还没有发现什么问题，则可以考虑安装。在安装之前，建议使用反病毒软件对下载回来的软件进行扫描，以免软件中包含其他不需要的内容。

在安装软件的过程中也要注意，虽然我们可能是从自己信任的地方下载的，并且经过搜索，发现所选择的版本没什么已知的问题，但这并不表示这个软件就是绝对安全可靠的。

很多人在开始学习计算机的时候，高手们往往都会这样说：装软件很简单，双击安装文件，然后一路"Next"就行了。于是很多人养成了安装软件时不检查可用选项、闷头安装的习惯。在目前不安全的网络下，如果我们安装每个软件都是这样操作的，可能系统中的灰色软件已经在泛滥了。

很多软件在运行安装程序的时候，首先会提供两个选项：快速安装和高级安装。如果选择"快速安装"，那么安装程序对于大部分非关键选项都将使用默认设置直接安装，只对一些关键的选项才让我们进行设置；如果选择"高级安装"，那么安装程序将会显示每个可用的选项供我们操作。为了避免被无意中安装了不需要的捆绑软件，建议从现在开始，改掉传统的软件安装习惯，不仅要使用"高级安装"选项，还要看清楚随后出现的每个选项。

也许觉得这样做纯粹是多此一举，事实也就是如此，很多不够"厚道"的厂商会把捆绑软件的选项用很小的字体放在很不起眼的地方，主要就是为了不引起我们的注意，达到

偷偷潜入系统的目的。当然这只是针对那些至少还提供了选项的软件，对于那些完全不提供任何选项，直接就把捆绑的软件自动安装到系统中的程序，如果条件允许，强烈建议不使用。

9.3.3 签名

前几年，对软件的安装程序进行数字签名的必要性还不是很明显，很少有人这样做。当时为了防范软件被感染了病毒，很多软件开发人员会在自己的软件下载页面上留下安装程序的校验码，例如 MD5 或者 SFV 校验码。

近年，数字签名技术得到了长足的发展，MD5 以及 SFV 等校验码已经很少使用了，因为数字签名更可靠，也更方便。那么这两种签名方式分别是怎么使用的？

9.3.3.1 校验码

前几年，网络环境不是很好，当时大家的网络速度普遍都很慢，从网络上下载文件的时候经常因为网络原因导致文件损坏，对于某些软件，可能损坏的文件依然可以运行，但在功能或稳定性上有缺陷。

另外一种情况，很多软件作者习惯找一些可以上传文件的“网络硬盘”，将自己的软件上传，然后在自己的个人主页、Blog 或者论坛上发布软件的下载链接，供大家从“网络硬盘”上下载。但文件作者担心自己上传的软件会被人恶意篡改或者捆绑病毒。

为了解决这种问题，当时很多人采用 MD5/SFV 校验码的方式保证文件的完整性。简单来说，这种校验码可以理解为文件的“指纹”，当对文件生成校验码的时候，专用的软件会自动读取文件内容的每个比特（计算机中存储信息的最小单位），并用特定的算法对读取的内容进行计算，生成一个字符串，这就是最终的校验码。因为所用算法的特殊性，只要文件的内容有哪怕一个比特的变动，都将导致文件的校验码发生巨大的变化。

因此，很多人在提供文件下载地址的同时，还会提供这个文件的校验码。用户下载了软件后，对下载回来的文件计算校验码，然后和文件作者提供的校验码进行比较。如果发现一致，则表示文件没有经过篡改；如果不一致，就需要注意。

另外一种方法更简单，文件的作者会提供校验文件。所谓校验文件，就是一个简单的包含了校验码的文本文件，不过扩展名不同（MD5 校验文件的扩展名是.md5；SFV 校验文件的扩展名是.sfv）。用户只需要将文件和校验文件下载到本地，然后使用验证软件打开校验文件，验证软件就会自动对目标文件进行计算，生成校验码，然后和校验文件中的比较，并报告比较结果。

现在虽然校验码已经用得很少，但依然有不少软件公司和个人在使用。因此，如果要下载的文件提供了校验码，可以按照本节介绍的方法在文件下载完毕后进行验证。

要对文件生成校验码或者直接打开校验文件进行比较，可以使用 HashCalc，这是一个免费软件，可以在这里下载：http://tinyurl.com/rsl8q，解压缩后需要安装。

运行 HashCalc 后可以看到图 9-52 所示的界面。首先在“Data”下拉菜单中选择“File”，然后单击右侧的“…”按钮，选择本地硬盘上要计算校验值的文件，最后选中要计算的校验值类型，并单击“Calculate”按钮。稍等片刻，所有选中的校验值就会显示在对应的文本框中。这里需要注意，我们常见的校验值有 MD5 和 SFV 两种，而 HashCalc 的界面上似乎没有 SFV 的选项，是因为 SFV 使用了 CRC32 算法，因此，只要选中“CRC32”，计算出来的校验值就是这个文件的 SFV 值。

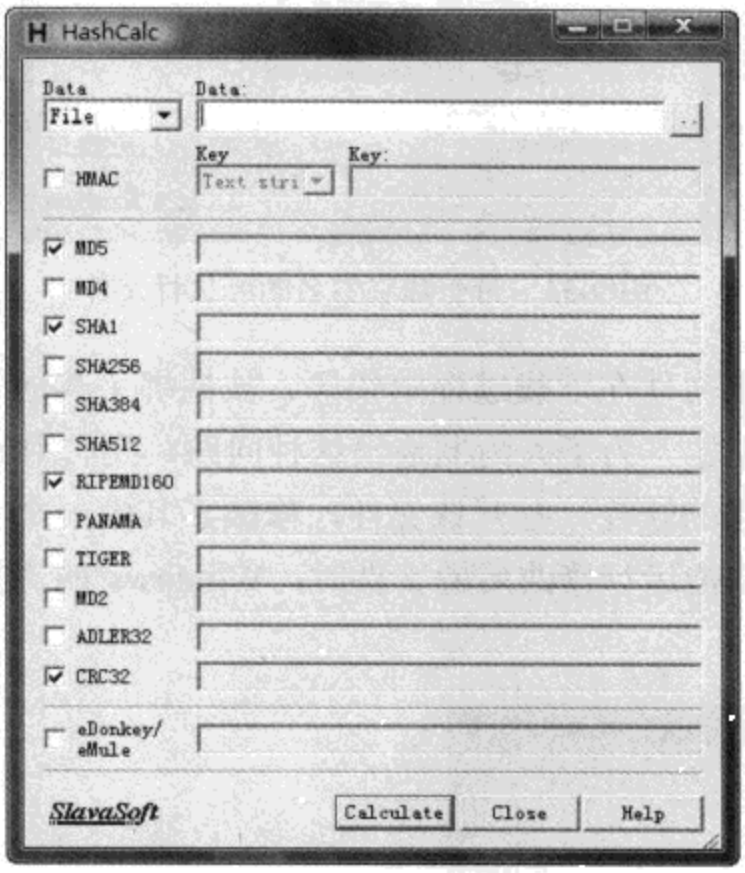


图 9-52　使用专门的软件计算文件的校验值

得到校验值后，与提供该文件下载地址的网页上显示的校验值进行比较，并确定自己下载的文件是否被篡改。如果发现结果不一致，可能是因为下载时出错导致的，请试试看重新下载，如果多次下载计算的结果一样，但都和网页上提供的不同，说明这个文件是有问题的。

9.3.3.2　数字签名

虽然校验码这种方式很好用，但现在已经逐渐被数字签名取代了。因为校验码只能确保一个文件在发布后没有被篡改，不能证明文件发布者的身份。而数字签名则可以同时实现这两个目的（有关数字签名的介绍请参考 9.1.2.1 节，虽然其中介绍的是用于网页加密的数字证书（签名），不过和用于文件签名的数字证书在原理和注意事项上都是一样的）。

当我们用 Internet Explorer 从网页上下载了一个可执行文件，并运行后，可以看到图 9-53 所示的界面，这表示该文件是带有数字签名的。

如果看到的对话框和图 9-53 所示的类似（对话框顶部显示为墨绿色，显示有“已验证的发布者”字样），就表示这个程序的数字签名有效，文件没有被篡改。如果希望看到有关

数字签名的详细信息，请在该文件上单击鼠标右键，选择“属性”，打开“数字签名”选项卡，从“签名列表”中选中厂商的数字签名，然后单击“详细信息”按钮，随后可以看到图 9-54 所示的“数字签名详细信息”对话框。如果在这里显示“此数字签名正常”，则表示该文件是没有被篡改过的，可以地放心打开它。

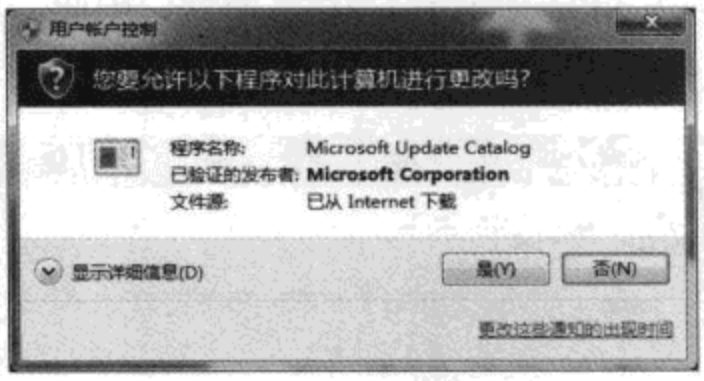


图 9-53　带有数字签名的可执行文件

下面假设情况：如果文件在下载过程中损坏、被捆绑了其他软件，或者被病毒感染，运行的时候会出现什么现象？为了人为制造出这种问题，我们用 eXeScope（一个可以修改可执行程序文件内部内容的软件）打开该文件，修改了其中一个字节的内容，并将改动的内容保存。当试图直接双击运行修改后的文件时，Windows 的“提示”对话框完全变成了如图 9-55 所示的样子。

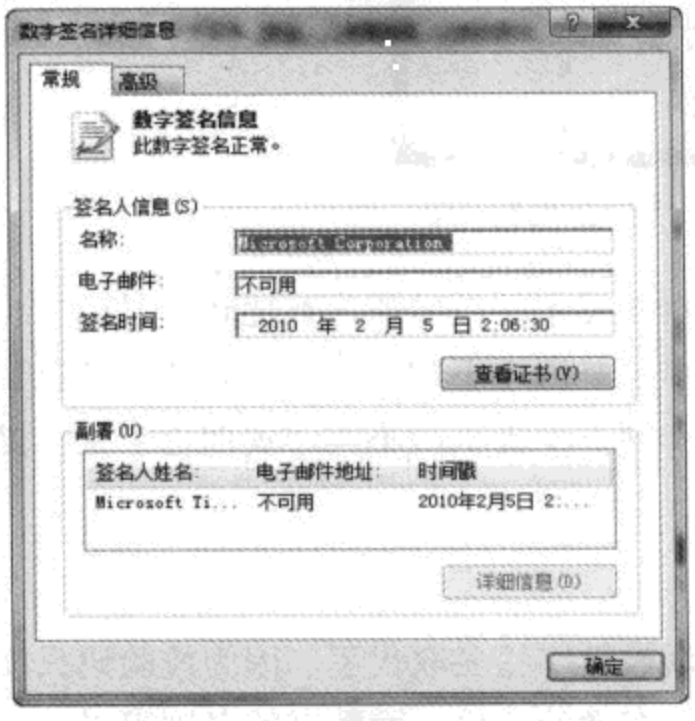


图 9-54　查看文件数字签名的详细信息

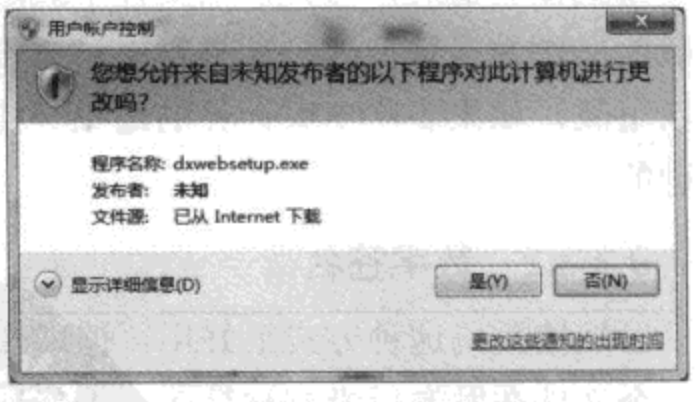


图 9-55　篡改导致文件的数字签名丢失

如果打开这个修改后的文件的“属性”对话框，会发现里面甚至根本没有“数字签名”选项卡，这进一步证明了因为修改导致文件的数字签名被破坏。

这里有一点需要注意，目前并不是所有的软件开发商都会给自己的程序添加数字签名，因此，如果单凭文件没有数字签名就说这个文件被篡改过，这是站不住脚的。好在已经有越来越多的软件开发商意识到了数字签名的作用，尤其是在 Windows 7 发布后，安装程序

中带有数字签名的软件也开始多了起来。因此，这个功能在一定程度上还是可以保证让我们下载到正确、可靠的软件安装程序。

9.4　防范通过 IM 软件进行的诈骗

在上文中，已经介绍了在网页上进行的钓鱼是怎么回事，然而钓鱼的手段多种多样，远非通过网页一种。因此，本节还将介绍其他常见的钓鱼方式，以及自保的办法。

9.4.1　社会工程学诈骗

提到“钓鱼”，我们不得不提“社会工程学”这个词，这个名词的真实含义远非字面给人的感觉那么高深。

举一个笔者遇到的例子。笔者平时主要使用两个聊天软件：A 和 B。有一天，一位朋友在软件 A 上跟笔者说，他家里有急事需要用钱，可自己正在开会，走不开，希望我能给他的银行账户里转一些钱。当时我就想过，这是不是别人在用他的聊天账号骗钱。但因为这位朋友本身就是在 IT 行业工作的，理论上应该不会在这种小事情上出问题，于是我打开了网络银行软件，输入账号，准备转账。而就在单击“确定”按钮前，我无意中看到他在软件 B 上登录了，软件 B 自动弹出了他的登录信息，并显示了他的名字，在他的名字后面显示了“我的软件 A 密码被盗了，不要给我转账”之类的字样。万幸，在最紧要的关头避免了进一步的损失。

所谓的社会工程学诈骗，就是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的手法。可以说，社会工程学诈骗跟计算机技术方面的知识没有太大联系，主要还是利用了人们在心理上的弱点进行的。社会工程学诈骗看似简单的欺骗，却包含了复杂的心理学因素，其可怕程度要比直接的技术入侵大得多。对于技术入侵，我们可以防范，但是心理漏洞谁又能时刻警惕呢？

有人可能会说了，你朋友的软件 A 账号被盗才导致别人借助他的身份行骗，难道盗取账号不需要计算机技术吗？话虽如此，可大家知道有多少人各种账号的密码只是简单的数字组合（生日、电话号码、特殊纪念日期）或者英文以及拼音字母（现成单词、自己或者亲人朋友的名字）？对于这样的密码，任何对我们的基本信息有所了解的人只要经过简单的尝试都可以猜测到。如果我们在所有的地方都使用同样的密码，那么密码被盗后的后果就是灾难性的。

基本上，除了上文中提到的仿冒网站以及钓鱼邮件利用了社会工程学原理进行诈骗外，我们遇到最多的还有通过各种 IM（Instant Messenging，即时信息）软件，例如 Windows Live Messenger、QQ 等软件中进行的诈骗。

下文主要针对在 IM 软件上常见的社会工程学诈骗方式进行介绍，并提出应对方法。

9.4.2 好奇心害死猫

前几年，一种名为“QQ 尾巴”的病毒现在几乎已经人尽皆知，虽然现在比较少见，可依然有人会上当受骗。这种病毒最先出现在 QQ 软件中，主要迹象是：中毒后，病毒会将一些信息主动发送给当前打开的 QQ 账号中的所有联系人。在发出的信息里包含了一些诱惑性的字眼，例如，“我发现一个在线看电影的网站，速度很快还免费，快来看吧”，并提供一个链接。收到这样消息的人可能觉得，这是自己的好友发来的，应该不会是骗人的信息。而一旦点击了对方发来的信息，就会访问一个带有病毒的网页，如果自己的系统中没有安装反病毒软件，或者浏览器的安全设置有问题，那么自己也会中毒。

除了“QQ 尾巴”，还有一种类似的诈骗方式：传输文件。现在的主流 IM 软件基本上都有文件传输功能，这类病毒就利用了这样的功能，一旦系统中毒，那么病毒就会将自己打包，然后发送给 IM 软件中的所有联系人。里面同样会有一些诱骗人的文字，例如，“这是我最新的照片，你快看看吧”。对方如果觉得这是自己好友发来的就轻易打开，自己就有可能中毒。

对于这类方式的诈骗，识别起来非常简单，只要询问对方是否给自己发送了文件或者链接就行了。因为这类病毒都是在用户不知情的情况下自动发送的，因此，如果对方说没有发送过这样的内容，那自然证明其中有问题。

另外一点就是，在充满风险的网络中，好奇心还是少一点比较好。有些人可能会觉得，既然朋友把这个网站或文件吹嘘得这么好，那我也看看吧，反正我还有反病毒软件，应该可以帮我拦截病毒。其实这就是一个很错误的想法，毕竟在目前的技术条件下，反病毒技术的发展依然是跟着病毒进化的脚步前进的，无论什么反病毒软件，如果没有更新病毒库定义，对于新出现的病毒可能都会不闻不问。虽然很多厂商宣称自己的软件具有类似“未卜先知”的主动查毒技术，但这类技术目前还很不成熟，也许通过这类技术真的可以查杀 1 个未知病毒，但很可能同时会漏掉另外 10 个。在涉及安全问题的时候，还是谨慎一些好。

因此，对于这类方式，只有一条建议：不要过分依赖反病毒软件，同时好奇心不要太强。

9.4.3 天上岂能掉馅饼

某天，我们可能会在一个网络游戏中收到了自称是“GM”（游戏管理人员）的消息，告诉我们说为了庆祝他们公司运营这个游戏 N 周年，公司举行了盛大的抽奖活动，我们已经被抽中一等奖，奖品是价值人民币多少元的游戏点卡，或者最新的某某型号显卡等。要想领取奖品，需要到“官方网站”去输入自己的游戏账号的用户名和密码进行身份确认，然后提供自己的地址，等到奖品邮寄过来。当我们兴冲冲地单击消息里的链接，到那个网站提交自己所有的资料后，可能马上就会发现，自己的网游账号因为密码错误无法登录了，就算自己申请过密码保护或者其他类似功能，待重设了密码，登录上去后可能会发现，自己辛苦打造的极品装备或者游戏币已经被全部盗走。

相对上面 IM 软件的例子，这种诈骗手法的技术含量更低，但是得手率是最高的。原因是什么？无非就是很多人都喜欢占便宜。因此，当遇到这类情况的时候不妨想一想，网上有那么多人，为什么便宜都来主动找我们。

要想识破这类伎俩其实也很简单，首先需要注意的是，无论任何时候，在遇到这类“好事”之前，最好能多想想，并通过各种方法求证消息的真伪。如果对“便宜”总是抱着“不占白不占”的念头，估计以后受骗的次数还会更多。

其次，如果真的要点击类似消息中提供的链接也请留个心眼。很多人可能纳闷了，在单击那些链接之前，我还注意了一下，确实是官方网站的链接，而且进去后的页面设计也是我所熟悉的，怎么能是假的呢？

我们以微软网站的域名“http://www.microsoft.com”为例来介绍这个问题。微软的域名大家都知道，可是大家觉得类似这样的地址：“http://www.microsoft.com@google.com”，访问的时候会带我们去哪里？当然，实际操作起来肯定不会这么明显，要隐蔽得多，例如，将“@”符号后面真正的域名用 IP 地址代替，或者用一些很罕见的域名后缀来实现，这样访问者看起来可能会将“@”后面的内容当做是网站页面的目录，而非真实地址。

不仅如此，还有一点很重要的，记住和自己关系比较密切的一些网站的真实地址。例如，笔者曾经见过这样的情况：有位朋友玩某个网络游戏时间很长了，因为偶尔要在网吧玩，他把自己的游戏账号申请了锁定功能，每次玩之前都要访问游戏运营公司的网站，对账号解锁，随后才可以登录游戏。这样做听起来很安全，可麻烦的地方在于，他虽然玩这个游戏都好几年了，但至今依然没有记住游戏运营公司的网站地址。那么他玩游戏之前怎样解锁账号？很简单的办法，启动游戏，在登录界面上有一个用于访问官方网站的按钮，单击这个按钮就可以调用浏览器打开官方网站。他觉得这个办法很方便，但笔者觉得是问题：如果系统中被安装了恶意软件，修改了这个按钮的真实作用，导致单击该按钮后会打开一个伪装成官方网站的盗号网站，而他没有察觉到，在盗号网站输入了自己的用户名和密码，后果会是怎样的？

因此，和在电子邮件以及网页上遇到钓鱼诈骗时的应对方法一样，如果收到了一些消息，需要提供自己的真实信息，宁愿稍微麻烦一些，亲手在浏览器的地址栏输入要访问的地址，也不要直接单击消息里面的超级链接。这样做虽然麻烦，但是要可靠很多。

CHAPTER

10

第 10 章　防范恶意软件

病毒、蠕虫和特洛伊木马程序一经感染，会给我们的系统带来很多麻烦，再加上过去几年里一些知名病毒的泛滥造成了重大的损失，因此，很多人对这类危险的防范很关注。虽然本书中前面的内容已经可以帮助我们将这类软件对系统的威胁降到最低，但有一个不得不承认的事实：反病毒手段往往都是跟着病毒制造技术的发展才提高的。例如，只有在知道了某个病毒的感染原理以及发作特点之后，才可以对系统采取一定的措施，防止被感染。因此，在做到了上文提到的所有内容后，依然不能大意，建议安装一个反病毒软件。

市面上有很多安全套装软件，同时包含了网络防火墙、反病毒、反间谍等功能，通常，安装一套这样的产品就可以保护系统防范各种网络威胁。如果愿意，也可以使用微软提供的安全产品。在 Windows 7 中，已经包含了 Windows 防火墙（有关 Windows 防火墙的相关介绍，请参考本书第 8 章）和 Windows Defender，另外，微软还提供了一个独立的反病毒软件 Microsoft Security Essentials（MSE），该软件可在微软网站上免费下载。我们完全可以使用 Windows 7 内建的，以及微软免费提供的安全软件，获得与市面上其他同类安全套装软件相同的保护，而且不用额外多花一分钱。

然而，保护系统安全并不是说安装安全软件后就可以万事无忧了，毕竟新的威胁层出不穷，甚至最近几年里每年发现的新病毒数量也越来越多，而安全软件如果不升级定义，对于大部分新的威胁都是无能为力的。所以，还要保证自己的安全软件能够经常更新，使用最新的定义。因为只有这样，才能最大限度地保护我们的系统和数据安全。

除此之外，很多人往往有一个误解，认为只要安装了安全软件，并经常更新定义，自己就可以高枕无忧了。遇到电子邮件中的附件，不假思索就打开；朋友在 IM 软件里发来了一个地址，就直接点击访问。这个做法是非常错误的。在计算机安全界有一种说法：整个系统在安全方面最薄弱的环节永远都是使用系统的人。老手可能不安装任何反病毒软件都不会中毒；新手也许安装了好几个反病毒软件，但系统里的病毒都可以开一间“病毒展览馆”。无论在什么情况下，良好的安全意识都是必要的，其次才是借助安全软件的辅助进一步保护系统。

目前市场上的安全软件种类很多，大家在选择的时候往往会面临很多困难。有些人习惯通过软件的认证来选择；有些人习惯在网上下载一些自称包含了上万个病毒样本的病毒

包，并用不同的软件检测，选择检测出来病毒最多的那个软件；更多的人则是人云亦云，别人说哪个好用就用哪个。

另外，很多人为了让自己的系统更加安全，往往会同时安装多个功能重叠的安全软件，这样做反而不好。因为安全软件大多工作在系统底层，和操作系统的结合相当紧密，如果同时安装多个此类软件，软件之间往往会产生冲突，轻则导致系统运行速度缓慢，重则可能导致系统无法启动或者频繁崩溃。

其实，哪个反病毒软件更好用，主要取决于个人的使用环境和习惯。本章将介绍微软免费提供的 MSE（在安装 MSE 后，Windows 7 自带的 Windows Defender 将被禁用，因为 MSE 本身同时包含反病毒以及反恶意软件的功能）。选择该软件的理由在于：

- MSE 是微软自家开发的，因此，和 Windows 系统的兼容性最好，通常不会与系统产生冲突。
- MSE 并不需要额外投资，而且有微软的强大技术后盾做支持，能够快速响应新出现的威胁。
- MSE 比较安静，并不会用喋喋不休的通知信息向我们宣告它的存在。只有遇到需要引起用户注意的问题时，才会用通知的形式告诉我们，平时都只是在后台默默地工作。
- MSE 的界面非常简单，并没有太多复杂的设置选项，但这绝对不意味着这个软件的功能简单。只不过为了照顾普通用户，该软件的大部分设置并不需要调整，即可很好地适应不同的使用环境，而且非常节约系统资源。

10.1　面对恶意软件

很多人可能对病毒、蠕虫、木马等程序比较熟悉，并且通常都了解一些防范这类程序的技巧。但实际上，最近几年，另一类威胁正在逐步显现，那就是恶意软件（也就是所谓的“流氓软件”）。这是一类非常特殊的软件，这类软件通常并不会对系统或者数据造成破坏（至少本意上并没有打算破坏），因此，按照常规的看法，这类软件属于正常软件，但因为这类软件往往利用一些非正规渠道（绝大部分病毒也会采取类似的方式）进入系统，非常隐蔽，而且难以彻底卸载，因此，具有病毒的某些特征。因为介于正常软件和病毒之间，因此，这类软件往往被称做“恶意软件”或者“灰色软件”，另外一些对这类软件深恶痛绝的人更是将其称之为“流氓软件”。对于这类不受欢迎的程序，也需要小心应对。

10.1.1　关于恶意软件

恶意软件都是怎么来的？

最开始，这些软件主要利用了 Internet Explorer 浏览器的 ActiveX 控件功能。因为这类恶意软件的开发商往往都具备一定的经济实力，因此，通常会花钱进行推广，例如，他们

会和一些访问量很大的网站合作，让这些网站在自己的网页上自动“推销”恶意软件，访客一旦通过这个网站安装了恶意软件，那么开发商就会给网站一定的经济回报。很多人因为不了解，只是看到自己熟悉的网站上在建议自己安装一个不知道是什么的软件，糊里糊涂就安装了，将“瘟神”请进了门，并产生“请神容易送神难”的局面。

这种方式的成功之处主要在于利用了人们不太警惕的心理。其实，每个人可能都会遇到安装 ActiveX 控件的要求，例如，在通过微软 Microsoft Update 网站进行更新的时候需要安装 ActiveX 控件；在浏览网页上的 Flash 之前需要安装 ActiveX 控件。因此，这就给很多人造成了一种错觉：为了实现网页上的一些特殊功能，就必须安装网站提供的 ActiveX 控件，否则网页将无法显示。因此，当他们看见自己经常去的网站要求安装 ActiveX 控件的时候，通常都会毫不犹豫地安装，殊不知，自己成了自己信赖的网站的赚钱工具。

后来很多人意识到了大部分网页上推销的 ActiveX 控件中的猫腻，开始抵制一些非必要的 ActiveX 控件，甚至很多热心人还编写了控件免疫程序，只要运行这种免疫程序，就会给推销控件的网页造成一种错觉，认为本机已经安装了这个控件。最多的时候，这类免疫程序通常能对上百种恶意控件进行免疫。因此，恶意软件的开发商也与时俱进，开始考虑通过其他方法推销恶意软件，这种方法至今仍然被广泛使用，那就是与共享软件捆绑。

其实，对于共享软件（一种软件销售模式，可以先试用，感觉满意再购买）中捆绑其他软件，大部分人还是抱有比较理智的态度的。毕竟，目前国内的共享软件大环境还很不成熟，很多人编写的优秀共享软件可能有大量用户在使用，但是愿意花钱注册的少之又少，于是很多共享软件的作者开始和恶意软件开发公司合作，给自己开发的共享软件中捆绑恶意软件，借此获得一定的经济回报。

对于比较厚道的共享软件作者，通常会在软件的安装过程中提供选项，用户可以选中选项，安装捆绑的软件；或者也可以反选选项，不安装捆绑的软件。但是对于少数共享软件作者，通常都会暗地里给系统中安装捆绑的软件。国内一家软件开发商曾经做过统计，这种捆绑方式最猖獗的时候，某个用于清理系统中垃圾的软件，里面捆绑的垃圾软件竟然多达 16 种之多（详见 http://tinyurl.com/ykyq3gk）。

10.1.2 恶意软件的危害

按理说，在安装一个软件的同时安装了其他软件也没什么坏处，这也是很多人的想法。但是“恶意软件”之所以被冠以“恶意”的名头，是有原因的。基本上，如果系统中存在下列问题，就证明系统中可能已经被安装了恶意软件：

- 系统的运行速度无缘无故地变慢，或者在没进行其他操作的时候，硬盘灯突然频繁闪烁。
- 刚登录到系统后，Internet Explorer 就自动运行，并显示广告网页。
- Internet Explorer 浏览器的地址栏中突然多出了一些涉及色情内容的链接。
- Internet Explorer 的工具栏上增加了一些陌生的按钮或菜单选项。

- Internet Explorer 的首页或者其他选项的设置被修改，并被锁定，无法恢复。
- Windows 桌面或者“开始”菜单中增加了一些不认识的软件的图标或者菜单项目。
- 原本工作正常的操作系统或者软件，突然开始工作异常。
- 登录 Windows 后，系统显示错误信息，告诉我们在加载一个.dll 文件的时候出错，或者没找到这个文件。

通常来说，恶意软件的危害主要表现在：

- 在用户不知情的前提下潜入系统。在自己的电脑中，任何未经我们批准就安装的软件（哪怕是有用的正常软件）都侵犯了我们的合法权益。同时为了避免用户卸载，这类软件往往会在系统中尽量隐藏自己的踪迹，甚至根本不提供能够彻底卸载的途径（有些可能提供有卸载程序，但根本无法彻底卸载）。
- 此类不必要软件的种类很多，并且往往具有同样功能的软件之间还会产生冲突，导致“流氓软件在系统中掐架，用户在一旁干瞪眼”的局面，不仅会影响系统的运行速度，还有可能降低系统的稳定性，甚至导致程序崩溃。比较轻的情况是，当我们在网上下载文件时，单击了文件的下载链接，也许会有四五个功能类似的下载软件争先恐后地跳出来，询问我们要将文件保存到哪里；而严重的情况，甚至可能导致软件崩溃，例如，当我们在论坛上花了半小时写一篇精彩的帖子，单击“发送”按钮的前一刻，浏览器就无端崩溃了。
- 这些软件通常会在 Internet Explorer 中添加一些自定义的内容，例如地址栏中的链接，或者工具栏上的按钮，或者 Internet Explorer 中网页右键菜单里的选项。笔者曾经见过的一个例子，一位朋友家里的系统中安装了太多不需要的软件，这些软件都给 Internet Explorer 的右键菜单中添加选项，所有这些选项已经多到导致在 Internet Explorer 中打开右键菜单后，菜单中的选项从屏幕最顶部显示到最底部都还没有显示完整。另外，为了吸引大家的注意，并吸引大家使用相应的功能，这些内容往往会使用一些诱惑性的字眼，甚至打色情擦边球。
- 虽然现阶段的恶意软件主要通过和其他软件捆绑的方式进行传播，但依然会将 Internet Explorer 看做是自己的大本营，基本上，几乎所有的恶意软件都会通过加载项的方式在 Internet Explorer 中添加自己的某些功能，这些加载项会随着 Internet Explorer 的启动自动运行。如果安装了太多的恶意软件，不仅会导致 Internet Explorer 的运行速度变慢，影响 Internet Explorer 的稳定性，同时还有可能造成泄密。举一个最简单的例子吧，我们在银行 ATM 机上取钱的时候，旁边站了一个陌生人，虽然他宣称不会偷看我们的密码，但谁会相信呢？
- 为了能够深入潜伏在系统中防止被卸载，很多恶意软件往往会采取 Hook（钩子技术，这种技术的概念比较难以理解，该技术可以让一个进程依附在另一个进程上运行，并影响被依附的进程。该技术的本意是为了实现更多正当的功能，但容易被滥用）或者加载驱动的方式入驻系统，而这些方式会对系统底层产生较大的影响，一旦产

生冲突或者出现其他问题，很可能导致系统蓝屏崩溃或者出现其他不稳定的因素。

10.1.3 防范恶意软件的一般原则

上文已经介绍了恶意软件的一些特征以及危害，那么如何有效地预防？如果被安装了恶意软件又该如何解决？

首先要明确的一点是，恶意软件之所以被称做“流氓软件”，很大程度上都是因为一旦安装了这些软件，它们就会在系统中扎根，通常情况下都很难彻底清理。而且因为各种恶意软件采取的潜伏技术多种多样，基本上没有什么通用的方法能够一劳永逸地解决问题。

虽然现在有很多专用软件可以清理恶意软件，但大部分软件被清理后依然会在系统中残留有痕迹。因此，首先应该从使用习惯上尽量杜绝“轻敌”的心理，尽量不要给恶意软件任何可乘之机。同时系统中要安装反间谍软件，并打开实时监控功能。这类软件可以监控我们日常的操作，一旦发现有恶意软件打算入侵系统，就会向我们提出警告。同时，这类软件还能在一定程度上清理系统中已经安装的恶意软件（但未必会很彻底）。

对于通过 ActiveX 控件的形式从网页上安装的恶意软件，首先需要注意的就是 Internet Explorer 的信息栏。在 Internet Explorer 6 发布之前，如果访问了需要安装控件的网页，Internet Explorer 会使用对话框询问用户是否安装，很多不明就里的用户直接就会单击“确定”按钮，在自己不知情的情况下将恶意软件装进系统。而且很多人在明知道不需要这个控件，但不得已必须安装的原因在于，老版本 Internet Explorer 中，如果网页试图安装控件，首先会检测系统中是否已经安装该控件，而这个过程会导致整个 Internet Explorer 长时间不响应（在网络速度慢的时候尤其严重），很多人不堪其扰，不得已才会安装不需要的控件。

在 Internet Explorer 6 SP2 以上版本中的情况就要好很多。默认设置下，如果在这些浏览器上访问了需要安装控件的网页，Internet Explorer 并不会直接显示询问是否安装的对话框，而是首先在地址栏上显示一个信息栏，里面列出了介绍性的文字（如图 10-1 所示）。要安装该插件，必须首先注意到信息栏的存在，并单击信息栏。

图 10-1 新版 IE 用信息栏取代了直接询问的对话框

实践证明，很多粗心的用户在实际使用中甚至根本没有注意到信息栏的存在，自然也就不会看到相关的安装选项。而且在新版本 Internet Explorer 中，在出现询问是否安装的信息栏时，实际上还没有检测系统中是否安装了该控件。因此，不会影响 Internet Explorer 的操作流畅程度。

我们如果足够细心，每次都能注意到 Internet Explorer 弹出的信息栏，那么在遇到类似图 10-1 的信息栏时，最好能多留个心眼。毕竟我们都知道，ActiveX 控件的主要作用就是为了支持网页上的一些特殊功能，而一旦网页本身都已经打开了，而且所有的功能都可以在正常使用的情况下，依然显示了一个黄色的信息栏询问是否安装某 ActiveX 控件的话，表明这个控件并不是显示网页所必需的，对于这种控件，自然是越少越好，能不装就不装。

通过上文介绍的方法，我们已经可以有效地避免恶意软件通过 Internet Explorer 浏览器入侵系统，然而恶意软件的入侵途径并非只有这一种，它们依然可能通过捆绑在其他软件中的方式进行入侵。因此，应该学会如何利用安全软件保护自己。

10.2　使用 MSE

由于 MSE 需要单独下载，因此，首先需要访问 http://tinyurl.com/yhe57cw，下载并安装 MSE。该软件的安装非常简单，没有过多的选项需要设置，并且安装好之后通常不需要重启动，即可生效。随后，如果双击该软件的桌面快捷方式，将能看到图 10-2 所示的主界面。

图 10-2　MSE 的主界面

这里有一个小提示，从上述地址下载的 MSE 版本可能并非最新。因此，在安装完毕后，最好能够单击图 10-2 所示窗口右上角“帮助”字样右侧的小箭头，从弹出菜单中选择“升级 MSE”，并在随后出现的对话框上单击“升级”。这样软件会自动检查程序本身以及定义文件是否有新版本。如果有新版本，还可以自动更新。

另外，由于 MSE 是微软自家的产品，因此，除了通过软件本身提供的更新功能升级定义外，还可以使用系统自带的更新功能升级软件和定义。所以，通常在安装该软件后，就不再需要担心升级的问题，因为这两套升级机制即可确保在任何时间，本机的 MSE 软件以

及定义都是最新版本的。

随后请注意软件窗口顶部的状态指示，在图 10-2 的例子中，显示了绿色的背景，并显示了“计算机状态-受保护”字样。在 MSE 中，可以通过不同于颜色的状态指示了解本机受到的保护情况：

- 绿色　计算机正在受到妥善的保护，所有的安全功能都已启用，未检测到威胁，并且所有的定义都是最新版本的。
- 橘黄色　计算机可能没有受到完整的保护，例如，某项功能可能被禁用或被关闭，或者定义文件不是最新的。
- 红色　计算机存在风险，例如，可能检测出感染了病毒，或者存在其他严重的问题，需要立刻处理。

10.2.1　实时监控

与其他任何安全类软件相同，MSE 也带有实时监控功能。这种功能会在后台自动工作，监控我们进行的各种操作，并从中找出可能存在的安全威胁。例如，在使用 Internet Explorer 从网上下载文件时，MSE 就会对下载的内容进行扫描，一旦发现其中存在风险，就会禁止访问下载的文件，并询问应该如何处理。如果使用电子邮件客户端软件收到包含病毒附件的电子邮件，MSE 也会适时发出警告，并提供不同的处理选项。

MSE 的实时监控功能可以监控多种不同的操作，例如，通过网络（局域网或互联网）获得的文件、收到的电子邮件、访问的网页等，一旦发现上述内容中存在安全威胁，那么，MSE 首先会将其拦截，然后向我们询问采取什么操作。

又如，当我们从互联网上下载了一个包含病毒的文件后，MSE 很快会检测到存在的风险，随后取决于具体的威胁类型，系统通知区域的 MSE 图标会变为橘黄色或红色，同时会显示图 10-3 所示的通知对话框。

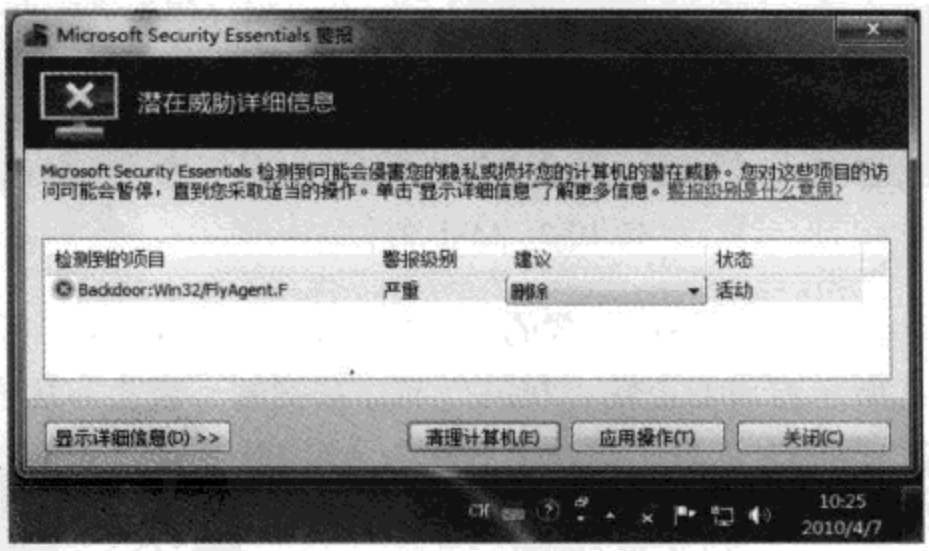


图 10-3　MSE 检测到活动中带来的安全威胁

默认情况下，MSE 会按照检测到的具体内容采取建议的操作。例如，如果检测出危险

的病毒，通常的建议操作都将是“删除”；如果是怀疑有问题的内容（通常可能是恶意软件），则可能建议进行“隔离”。因此，此时可以单击“显示详细信息”按钮，查看检测到的具体问题，然后结合实际情况采取需要的操作。

对于建议的操作，如果和自己预期的目的不一致，还可以通过“建议”下拉菜单选择其他操作。例如，可以选择“隔离”，这样有问题的内容不会被彻底删除，而是被移动到 MSE 的隔离区中，稍后我们可以自己处理相关问题。如果确信 MSE 检测的问题是不存在的，被怀疑的问题是安全的，此时也可以选择“允许”，这样，MSE 将忽略该文件可能存在的风险（对于普通用户，强烈建议不这样做）。选择好所需的操作后，单击“应用操作”按钮，即可对检测到的内容应用建议的，或我们自己选择的操作。

操作执行完毕后，如果 MSE 的通知对话框背景色变为绿色，则证明威胁已经彻底清理，可以放心使用计算机。但如果背景不是绿色的，则意味着系统中依然存在安全隐患，例如，可能是病毒清理不彻底，或者有其他问题。此时最好能对整个系统进行一次彻底的扫描，具体方法会在下文介绍。

对于检测到的威胁，如果想要了解更详细的信息，还可访问微软恶意软件防护中心：http://tinyurl.com/ngo9pq。

如果因为某些原因，MSE 将可能存在风险的内容删除或隔离，但我们希望将其恢复出来，则可以按照下列步骤操作：

STEP 01 打开 MSE 的主界面，单击“历史记录”选项卡。

STEP 02 选择“隔离项目”，随后所有被 MSE 隔离的内容都会显示在下方的列表中（如图 10-4 所示）。

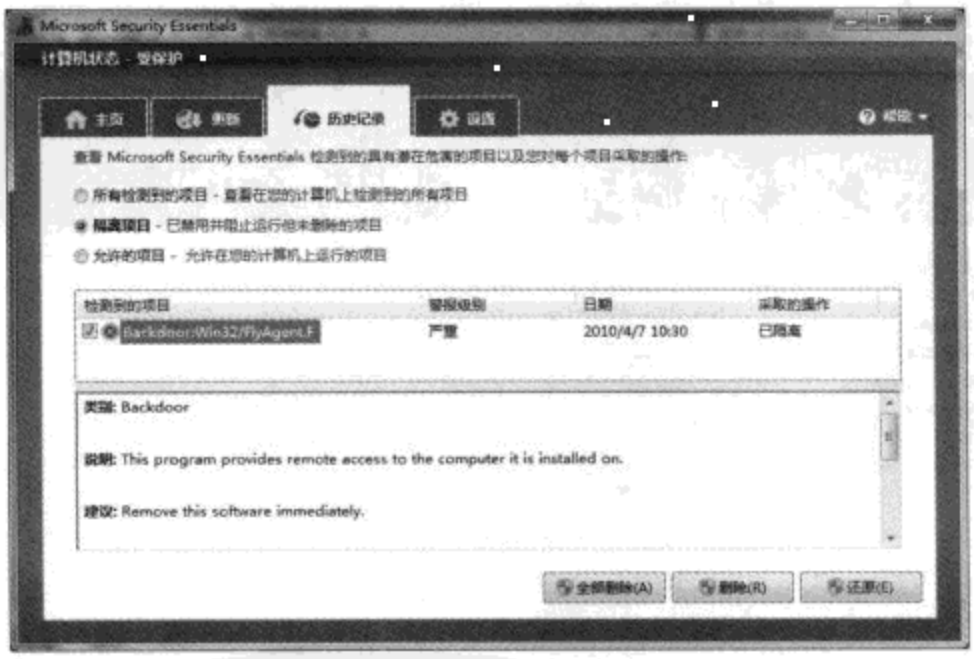


图 10-4　还原被 MSE 隔离的项目

STEP 03 对于希望恢复的内容，单击对应的复选框，将其选中，然后单击“还原”按钮即可（请确信被还原的内容是因为误判才被隔离的，如果还原有风险的内容，可能会导致更麻烦的后果）。

STEP 04 如果希望将隔离区清空（可以释放被占用的硬盘空间），则可以选中所有不再需要的内容，然后单击“删除”；或者直接单击“全部删除”，将隔离区的所有内容都彻底删除。

10.2.2 扫描

通常情况下，MSE 的实时监控功能就可以确保系统安全，但有些时候我们可能依然需要手工执行一些扫描。例如，每隔一段固定的时间，对整个系统进行彻底的扫描；或者在将别人的可移动存储设备（例如 U 盘）连接到自己的计算机后，对这些设备进行扫描；或者在执行某些操作后，对硬盘上的特定位置进行扫描。

如果希望扫描整个系统（建议每月或者每周执行一次），可以按照下列步骤操作：

STEP 01 打开 MSE 的主界面，在窗口右侧的扫描选项中选择“快速”或“完全”。

STEP 02 单击“立即扫描”。

对于“快速”和“完全”这两种扫描方式，将鼠标指针指向后，即可了解这些方式的区别，以及适用的场合。通常，快速扫描更加迅速，但不是很彻底。因此，可以根据实际情况选择要使用的扫描方式。

如果希望对某个可移动存储设备、某个硬盘分区，或者特定的文件或文件夹进行扫描，则需要用 Windows 资源管理器显示代表扫描对象的图标，用鼠标右键单击它，选择“使用 MSE 扫描”。

默认情况下，MSE 会在每周日的凌晨对整个系统进行扫描，如果希望更改扫描的计划时间，或者修改具体的扫描参数，则可以在 MSE 主界面底部单击“更改我的扫描计划”，随后可以看到图 10-5 所示的界面。

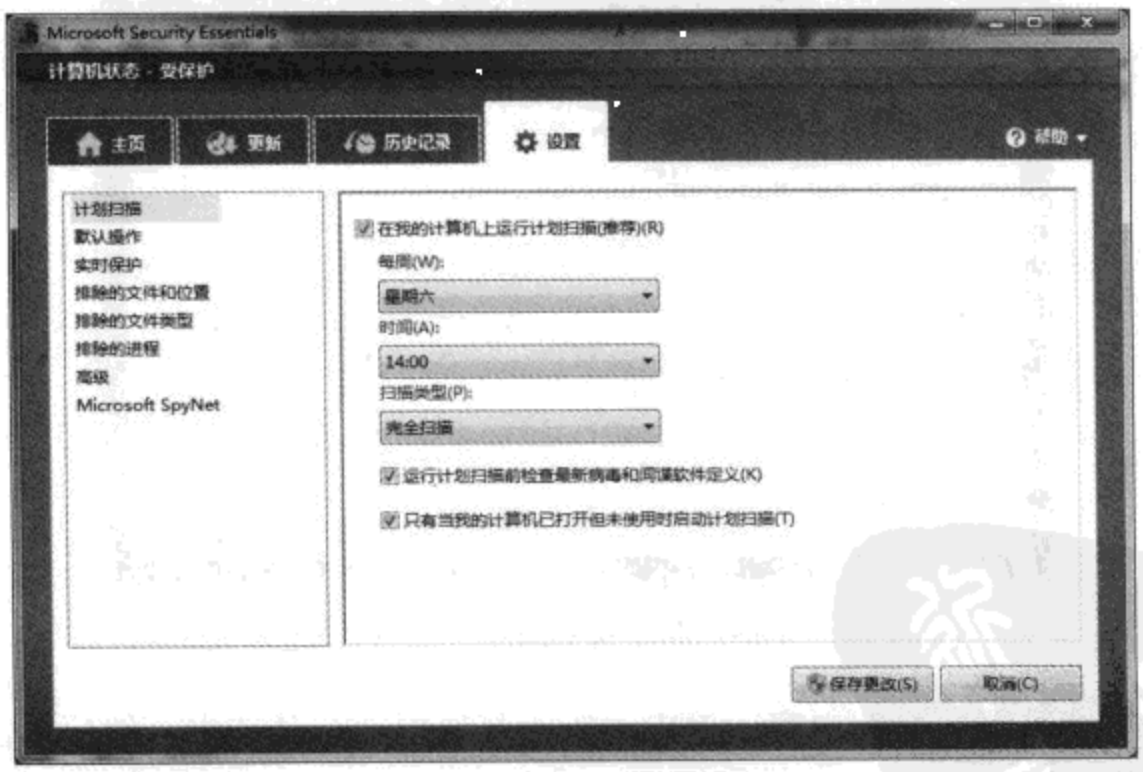


图 10-5 更改自动扫描的计划

如果不希望自动进行定期扫描，可以反选“在我的计算机上运行计划扫描”选项。如果希望使用，但希望修改计划的扫描时间和扫描模式，则可通过下方的选项指定。在这里需要注意，建议选择计算机已经打开，但不常使用的时间。例如每周例会的时间，或者午餐时间，这样可以将扫描操作对工作的影响降到最低。

在该界面底部还有两个选项，建议都选中。对于“运行计划扫描前检查最新病毒和间谍软件定义”选项，在每次计划扫描开始之前，MSE 会首先检查是否有新版本的定义文件可用，这个选项可以确保每次的计划扫描都使用了最新的定义，进一步提升检出率。

如果选择“只有当我的计算机已打开但未使用时启动计划扫描”，那么一旦某次计划时间的计算机被关闭，下次启动的时候，MSE 将不立刻进行扫描。例如，很多人觉得不方便的一点：计划了每周在某个时间进行扫描，但有一次扫描时间里因为停电，没有开机。等到来电后，原本积累了大量工作，需要立刻处理，但此时 MSE 正在忙于漏掉的计划扫描，导致其他工作受到影响。但如果选中该选项，那么一旦某次计划扫描由于系统关闭而漏掉，下次开机的时候，MSE 并不会立刻开始执行漏掉的扫描。

10.2.3　修改 MSE 的选项

MSE 提供的配置选项并不多，而且默认的设置已经可以满足大部分人的需求。如果有必要，也可以结合实际情况修改 MSE 的选项。在 MSE 主界面上单击“设置”按钮，随后可看到所有可供设置的选项。

1. 修改建议操作

针对检测到的不同危险程度的内容，MSE 可提供默认的操作。例如，如果检测到病毒，通常的默认操作都是删除；如果检测到恶意软件，默认的操作可能是隔离；如果检测到其他不严重，但可能危害隐私的内容，默认的操作可能会是“隔离”或者“允许”。

这些默认操作都是根据 MSE 的定义文件决定的。微软的恶意软件防护中心在捕获到新的威胁后，通常会对威胁进行评估，判断危险程度，然后根据危险程度分配一个建议的操作。对于一般用户，通常使用默认的建议操作即可保护系统防范各种危险。

如果因为某种原因，希望使用自定义的默认操作，也可以通过 MSE 提供的选项进行修改。在设置界面左侧的列表中单击“默认操作”，随后即可在右侧窗格看到图 10-6 所示的内容。

在修改前需要明确下列问题：

- 针对不同级别的警报，一旦修改建议的操作，则该级别的所有内容都将应用我们所选择的建议操作。
- 虽然不同警报级别的默认操作可以修改，但警报级别是由微软恶意软件防护中心定义的，用户无法修改。例如对于某个病毒，如果微软将其定义为“严重警报”，就只能采用针对严重警报级别设置的建议操作。

- 针对不同的警报级别，可采用的建议操作会有所不同。例如对于严重警报，就无法使用“允许”作为建议操作。

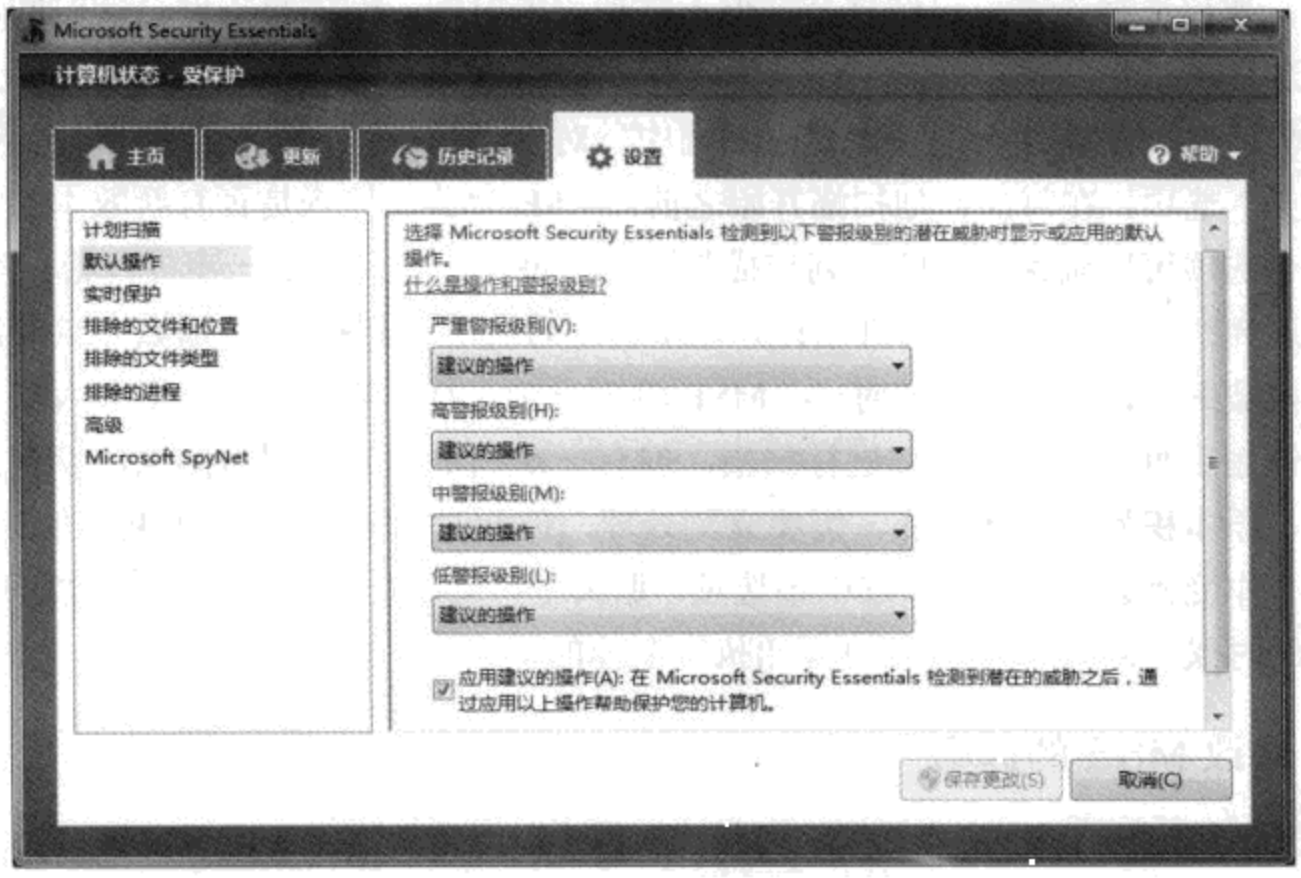


图 10-6　查看和修改默认的建议操作

针对不同的警报级别，从下拉菜单中选择要使用的建议操作，然后单击“保存更改”按钮即可。另外需要注意，如果不希望 MSE 执行建议的操作，而是在遇到任何警报之后都通知我们，并询问要采取的操作，则可以反选“应用建议的操作”。这样我们就能对 MSE 所采用的操作进行全面的控制。但有时候如果威胁太多，可能会非常烦人，甚至频繁打断其他工作。

2．使用排除功能

在某些情况下，我们可能明知某个文件存在风险，但依然希望能够打开。例如，研究人员可能希望研究某个病毒的特征，而需要在测试环境中执行，此时可以配置 MSE 的排除功能。排除功能的含义是：一旦通过某些规则定义了排除，那么，就算 MSE 检测到危险的内容（哪怕是最高级别的危险），只要内容符合排除规则，MSE 就不会对该内容采取任何操作。

这种做法可能会导致很严重的安全隐患，在此建议慎用。对于普通用户，建议只有在存在误报情况时才进行排除。例如，自己公司开发的一个重要软件，由于某些原因被 MSE 误报为病毒。在 MSE 的定义文件升级之前，为了正常使用该软件，就可以将该软件中被误报的组件或者整个软件的安装目录添加到排除列表中。

MSE 支持通过具体的文件、路径或文件类型，以及进程添加排除。这些内容分别需要在“排除的文件和位置”、“排除的文件类型”，以及“排除的进程”下设置。以上文的例子来说，假设企业中必须使用的某个软件的可执行文件 app.exe 被 MSE 误报为病毒，为了使

用排除功能，此时可使用“排除的文件和位置”功能。

如图 10-7 所示，在 MSE 的设置界面进入该节点，并在右侧窗格中通过“添加”按钮指定 app.exe 文件的完整路径，最后单击“保存更改”按钮即可。

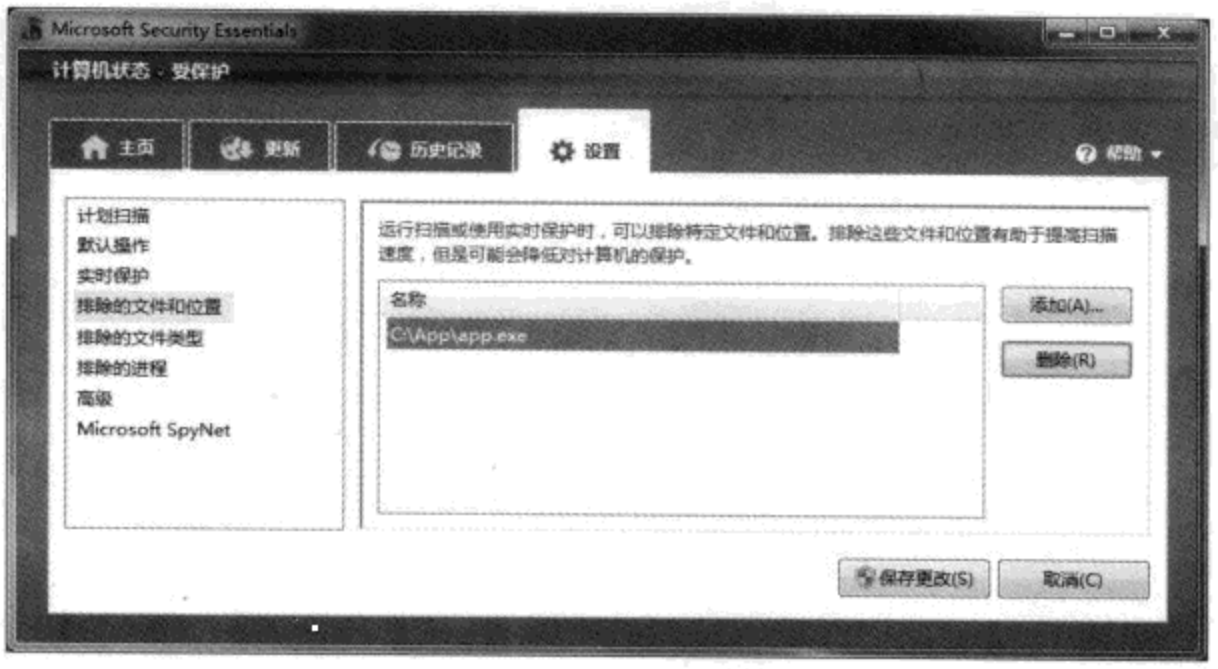


图 10-7　为 MSE 设置排除

4

第 4 部分
其他安全问题

通过对前三部分的阅读，我们应该了解了在使用 Windows 的过程中需要注意的大部分安全问题。只要能够按照上文提供的建议进行操作，Windows 的安全性将会更高，而且计算机中保存的重要数据也更妥善。

然而，依然有很多问题是我们需要面对的。例如，家里有儿童也需要使用计算机，那么如何保护儿童不会受到网络上各种不良信息的影响，同时能够引导儿童更加健康、合理地使用计算机？如何保护系统不受脱机方式的攻击？如何有效地备份特定的文件、文件夹、系统状态，甚至整个系统，并在系统出现问题之后正确还原？这些内容将在本部分介绍。

CHAPTER

11

第 11 章　家长控制

现在有计算机的家庭越来越多，甚至很多家庭已经有多台计算机，几乎所有的家庭成员都会使用计算机处理日常生活中的各种问题。这时候，新的问题也来了。

孩子放暑假了，按理说，经过一个学期紧张的学习，在假期让孩子用计算机进行娱乐，放松自己，这无可厚非。可家长都要上班，如何有效地避免孩子长时间沉迷于网络游戏或者聊天？

孩子平时需要在网络上搜索资料，完成家庭作业，但如何在允许孩子访问网络的同时限制对特定内容的访问？

一些家长可能平时也想玩游戏，释放工作中积累的压力，但是有些游戏因为过于血腥或者暴力，是不适合孩子玩的。如何限制对于某些游戏只允许家长运行，而禁止孩子运行？

如果你已经在使用 Windows 7 操作系统，就可以充分享受到这一功能带来的便利。

11.1　家长控制功能使用的前提条件

要使用“家长控制”功能，首先要做的就是分别为孩子和父母创建独立的用户账户（这通常都是父母们容易忽视的）。对于基于 NT 架构的 Windows XP/Vista/7 操作系统，多用户账户功能是一个重要改进，在这些系统中，每个人可以建立自己的账户，进而在不影响其他账户设置的情况下对自己的使用环境进行自定义的设置。然而很多人可能还习惯于 Windows 9x 中传统的单用户环境，全家人使用一个账户，这样既不能发挥多用户操作系统的优势，也不能进行彻底的限制。

因此，在继续之前，首先需要为父母和孩子创建不同的账户，孩子的账户最好属于标准账户，而父母的账户可以是管理员账户，同时需要用密码保护，以免孩子使用父母的账户登录来解除限制。关于账户的创建和密码的设置，请参考本书 2.1.1 节的相关内容。

需要注意的是，虽然在开发该功能的时候，微软已经将其进行了尽量的简化，家长的所有设置都相当简单、明了。但是目前的实际情况是，在绝大部分家庭中，父母的计算机技术水平往往不如自己的子女。因此，如果在设置上存在疏漏，可能导致不仅没有把子女“限制”好，反而使自己的活动受到了子女的“限制”。例如，父母可能给自己创建了管理

员账户，并设置了密码，但密码很简单，就是自己的生日或者家里的电话号码，对于这样的密码，只要对父母有所了解的人都可以猜到，更何况是自己的孩子。因此，密码的安全性也很重要。关于如何创建安全密码的方法，请参考本书 1.3.1.3 节。

本书中下面的内容会使用两个账户，其中名为“家长”的账户是管理员账户，供父母使用，设置有强密码；名为“孩子”的账户是标准账户，供孩子使用，没有设置密码。在创建好各自的账户后，需要按照下列步骤启用家长控制功能：

STEP 01 在“控制面板”中依次单击“用户账户和家庭安全”→“家长控制”。

STEP 02 首先需要对家长控制功能的一些全局选项进行设置，单击窗口左侧任务列表中的“游戏分级系统”链接，随后可以看到图 11-1 所示的界面。

图 11-1　选择要使用的游戏分级系统

STEP 03 游戏分级系统是用于判断游戏内容，以及适用人群的重要信息。很多国家和地区都有专门的机构给在本地销售的游戏进行评级，评级信息会被标示在游戏的包装盒上，供用户在购买的时候参考。同时对于新的全面支持 Windows 7 的游戏（这一标准叫做 Games For Windows，详细信息可参考：http://tinyurl.com/y8uugyp），游戏的安装文件中也会有用于提供分级信息的功能。然而遗憾的是，虽然国内有机构叫喊要给游戏分级已经喊了多年，但是这方面的应用一直没有什么太大的进展。因此，在这里只能使用国外的游戏分级信息，例如，默认的 ESRB（美国娱乐软件分级委员会）系统，当然，这些系统也就只能对在美国市场上销售的游戏生效。

STEP 04 选择了分级系统后，还要安装用于实现网页过滤和活动报告的控件，请访问 http://tinyurl.com/yd8om74。这是一种开放的平台，任何公司或机构都可以根据需要，编写出不同的家长控制控件，并在网上提供下载。在撰写本书时，只有微软提供的 Windows Live

家庭安全控件[①]可供使用，而为了使用 Windows 7 的家长控制功能对孩子的网商活动进行限制和控制，必须首先安装该控件。下文将以 Windows Live 家庭安全控件为例进行介绍。

下载 Windows Live 套件的安装文件，并在图 11-2 所示的要安装的组件界面中，确保选择了“家庭安全设置”组件，并完成其余安装操作即可。

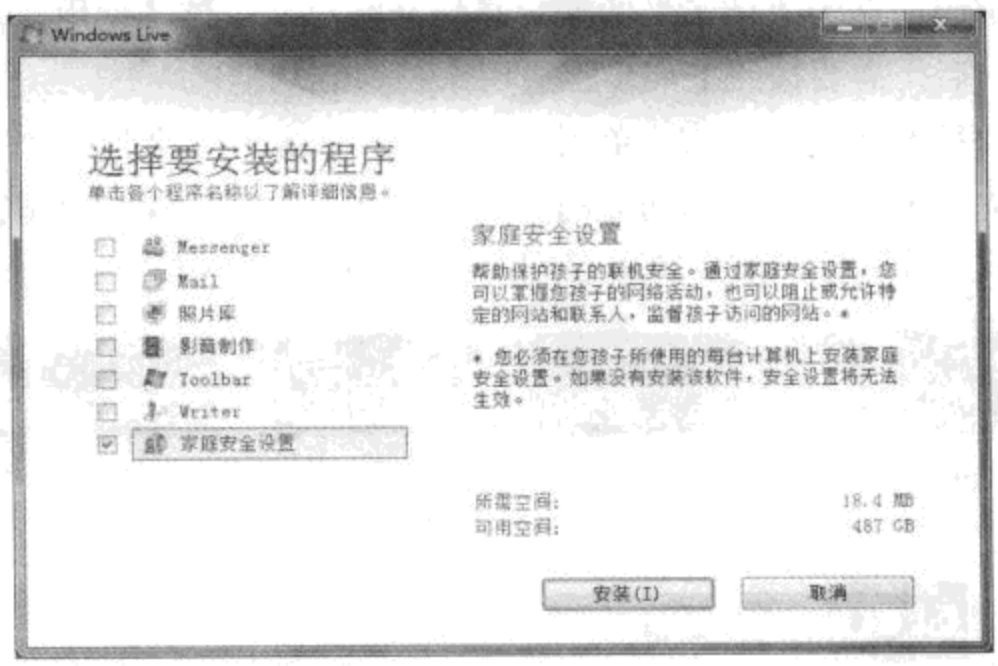


图 11-2　选中“家庭安全设置”组件

STEP 05 安装完毕后，如果一切无误，在控制面板的家长控制设置页面的底部，应该能看到类似图 11-3 所示的提供商。

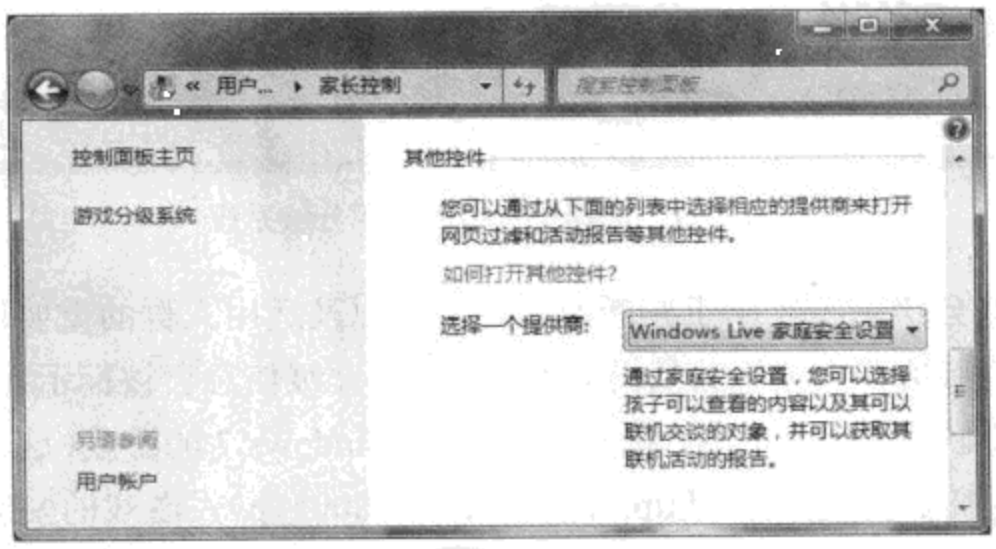


图 11-3　安装好的提供商程序

至此，家长设置功能的全部选项就设置完成了，我们可以启用家长控制，并根据需要启用不同的限制。方法如下：

STEP 01 在“控制面板”中依次单击“用户账户和家庭安全”→“家长控制”。

① 该控件实际上已经包含在 Windows Live 套件中，因此，也可以直接在 Windows Live 套件的安装程序中选择安装这一组件，可在 http://get.live.com 中下载。

STEP 02 随后系统需要我们选择想要控制的账户，这里直接单击“孩子”账户即可。由于安装并使用了 Windows Live 家庭安全设置控件，还需要使用家长的 Windows Live ID 登录，这样，家长日后就可以在任何一台可上网的计算机上监控孩子的使用情况。因此，请使用家长的 Windows Live ID 登录。但是需要注意，如果安装了其他提供商的程序，则具体的做法可能会有所不同。

STEP 03 接下来可以看到图 11-4 所示的界面，在这里需要选择受监视的 Windows 账户，本例中，选择“孩子”账户即可。选择完毕后单击“保存”按钮。

图 11-4　选择要监视的账户

STEP 04 等待片刻，单击“关闭”按钮。随后将返回到图 11-5 所示的家长控制主界面，在这里需要选择“启用，应用当前设置”选项。

STEP 05 接下来需要通过“Windows 设置”选项下提供的三个链接针对对应的内容设置限制。具体的做法会在下文中介绍。随着每个选项的设置，在图 11-5 所示界面右侧的“当前设置”一栏会显示设置内容的概述。

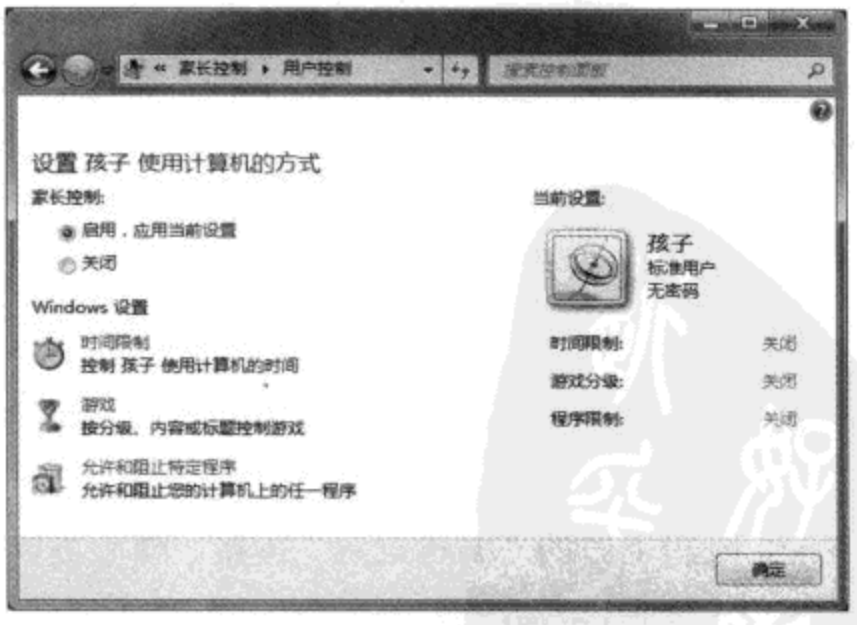


图 11-5　启用对其他 Windows 功能的限制

STEP 06 如果觉得所有需要的选项都设置好了，可以单击“确定”按钮保存设置。如果还有其他账户需要设置，则可以再次重复上述过程。

11.2 启用和设置家长控制

下面我们会分别针对不同功能的操作进行介绍。

11.2.1 设置可访问的网页内容

首先需要对孩子可访问的网页以及联系人信息进行限制和监控。由于在 Windows 7 中，该功能是通过额外安装的 Windows Live 家庭安全控件实现的，因此，所有的设置都需要在 Windows Live 网站上进行。这样做的好处主要是，家长即使不在家里，也可以通过任何一台可联网的计算机对孩子的使用情况进行实时的限制和监视。

具体做法如下：

STEP 01 使用 Internet Explorer 浏览器打开 Windows Live 家庭安全设置网站：http://familysafety.live.com，并使用家长 Live ID 登录。这里需要注意，登录所用的 ID 必须与图 11-4 中操作时登录的 ID 一致。如果一切无误，应该能看到图 11-6 所示的界面，请留意界面中至少应该有一个“家长”账户和一个“孩子”账户。如果需要添加其他家长账户或孩子账户，可以单击对应的链接，并按照提示进行操作。

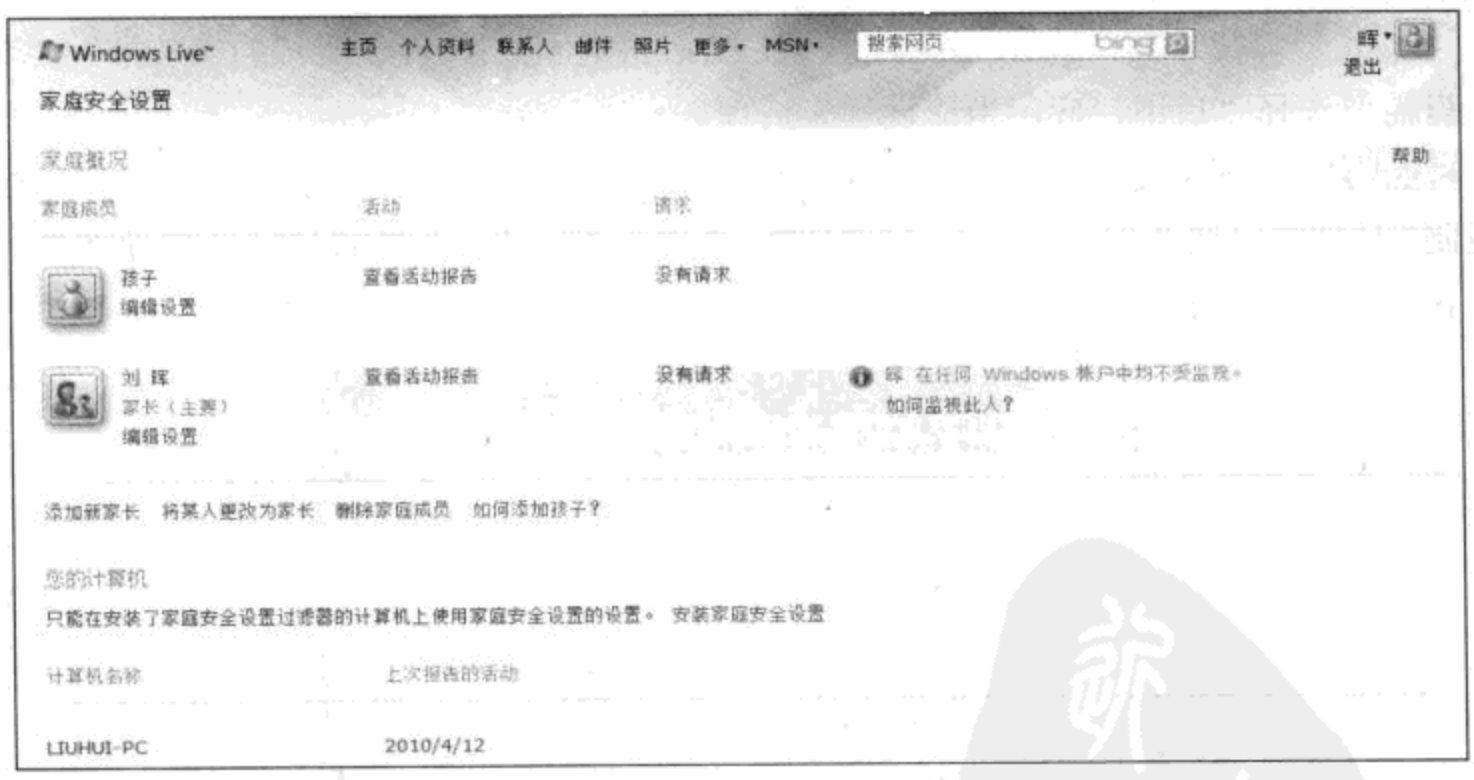


图 11-6 通过网页管理孩子的在线活动

STEP 02 单击“孩子”账户下方的“编辑设置”链接，随后可以看到孩子的设置界面，这里列出了 4 种功能，下文将分别进行介绍。

STEP 03 如果希望对孩子可浏览的网页类型进行限制，需要单击“网页过滤”链接，

随后可以看到图 11-7 所示的设置页面。

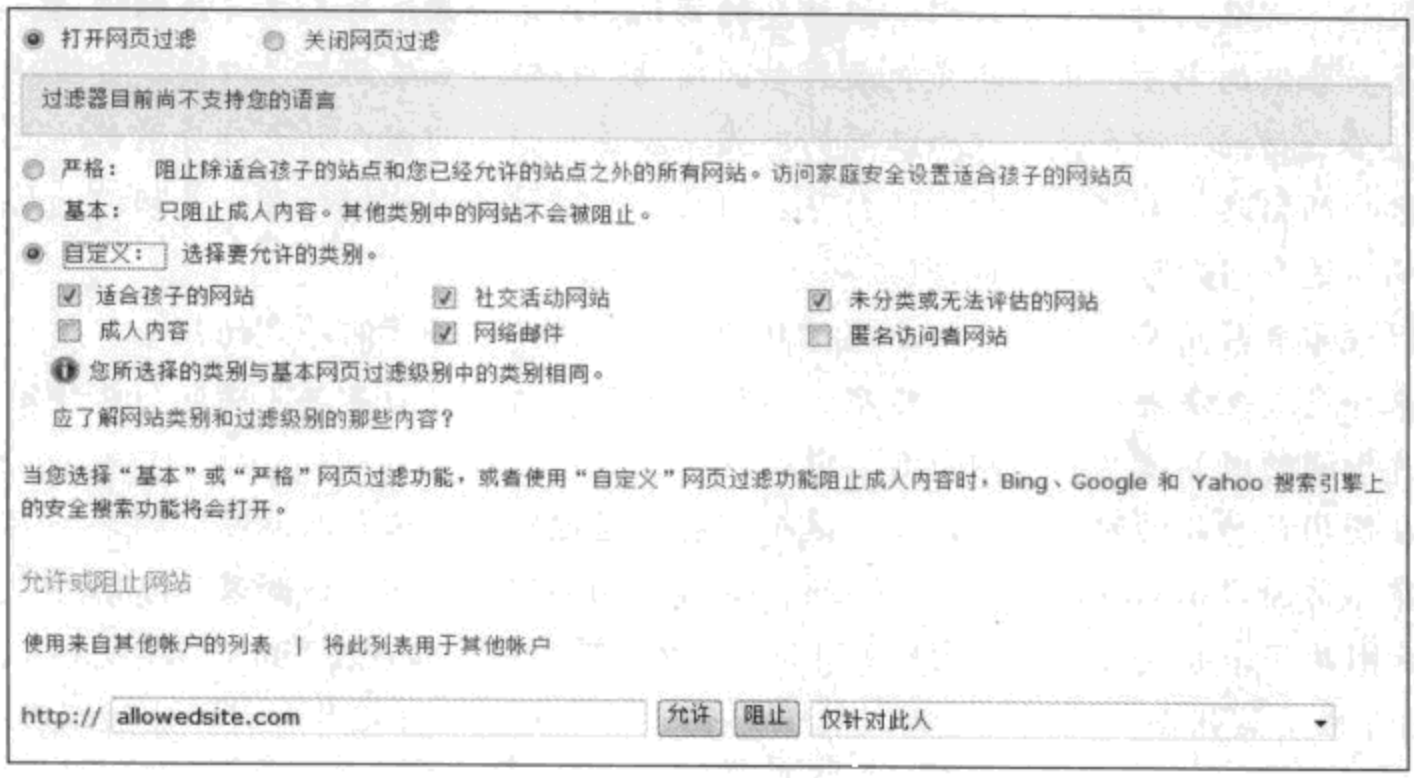


图 11-7　对网络活动进行限制

STEP 04　首先需要选择“打开网页过滤”，并在该选项下方选择过滤的严格程度。这里提供了三个选项，其含义分别如下：

- **严格**　如果选择该选项，则除非某一网站明确表明自己是针对幼儿的，否则一律被禁止访问。在使用该选项后，还可以手工指定某些允许访问的网站。这通常是最严格的限制选项。
- **基本**　如果选择该选项，则只有所访问的网站包含成人内容时，才会禁止孩子浏览，其他类型的网站都将畅通无阻。
- **自定义**　如果选择该选项，则可以根据不同的类别选择允许孩子访问的网站。

STEP 05　设置要过滤的级别后，还可以在“允许或阻止网站”选项下手工指定黑白名单。如果希望将某一网站添加到黑名单中，可以输入域名，并单击“阻止”，这样就算这个网站按照上述等级是适合孩子访问的，也将被禁止；单击“允许”，则可将网站加入白名单，这样就算这个网站按照上述设置是不适合孩子访问的，孩子也可以顺利访问。

STEP 06　将页面向下拖动，还可以看到一个有关文件下载的选项，该选项决定了孩子账户是否可从互联网上下载文件，该选项需要根据实际情况进行设置。

STEP 07　设置完所有的选项后，单击“保存”按钮。

窍门　**“未分类或无法评估的网站”是什么意思？**

在图 11-7 所示的界面中，选择“自定义”级别后，将看到一个“未分类或无法评估的网站”的选项，这是什么意思？其实，对网页的内容进行筛选这个功能是通过网站提

供的分级信息，以及 Windows Live 家庭安全功能的人工筛选来判断是否允许孩子访问特定网页的，那么，对于没有提供分级信息的网站，或者尚未进行人工筛选的网站，又该怎么办？如果选中了“未分类或无法评估的网站”选项，如果网站没有提供分级信息，系统将禁止访问。但在使用这个选项的时候需要注意，因为国内的大部分网站（无论提供什么样的信息）都很少提供分级信息，因此，选择该选项可能导致正常网站的访问受到影响。这个问题可以这样解决：

假设希望禁止其他没有提供分级信息的网站，但是允许访问特定的几个，则可以反选“未分类或无法评估的网站”选项，然后使用下方的“黑白名单”功能，将特定的几个允许访问的网站域名加入到白名单中。

在使用该功能的时候需要注意，这个功能是通过域名来识别网站的。例如，假设只允许孩子访问“http://www.microsoft.com”域名，当然可以实现。但如果这个网站上的某个页面引用了来自其他网站的内容，例如，其中的某个图标保存在“http://www.msn.com”域名下，或者这张图片的路径是网站域名的 IP 地址，那么这张图片也将无法显示。另外，在输入域名的时候也需要注意，假设希望禁止孩子访问“site.com”站点，最好输入“site.com”进行限制，而不是输入“www.site.com”进行限制，因为“site.com”涵盖了该域名下的所有子域名，也就是说，只要是以“site.com”结尾的域名都会被包含在内，如果使用“www.site.com”，则诸如“mail.site.com”这样的二级域名就不会被包含在内。

经过上述设置后，孩子在浏览网页的时候将只能访问提供的分级信息符合需要的网站，或者在允许的网站列表中添加的网站。其余网站的访问都会受到限制。

11.2.2 设置可用时间

孩子的自控力比较差，经常会长时间沉溺于游戏或者网络中，而做父母的也不可能天天守在电脑前监视孩子，这时候就可以使用 Windows 7 中的账户登录限制功能来设置允许孩子的账号登录的时间，进而达到限制使用的目的。

在图 11-5 所示的界面中单击“时间限制”链接后，可以看到图 11-8 所示的界面，在这里可以限制孩子的账户什么时候才允许登录，并且决定允许使用的时间。

在该界面中，一周七天、每天 24 小时的时间段都用方格表示了出来，蓝色的方格代表禁止孩子使用计算机的时间，而白色的方格则是允许孩子使用的时间。例如，我们希望设置让孩子的账号在一周七天里，每天都只有下午五点到七点可以使用计算机，其他时间都无法使用，就可以通过拖动鼠标的方法将不允许的时间都拖选出来，实现限制。

11.2.3 设置可玩的游戏

在上文中介绍了如何选择用于限制游戏的分级系统，那么具体该如何进行限制？这时候可以在图 11-5 所示的界面上单击“游戏”链接，打开图 11-9 所示的界面。

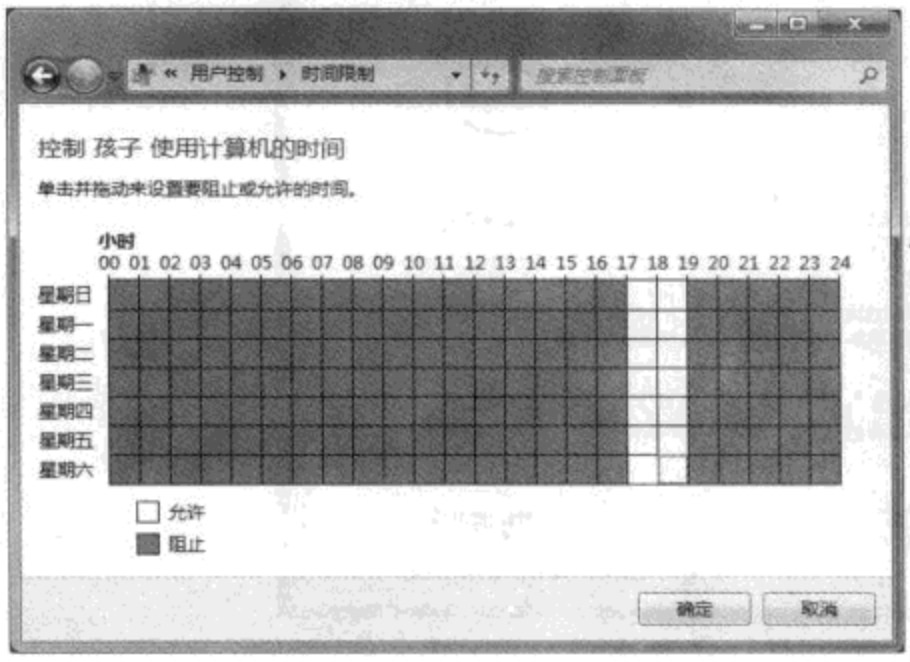


图 11-8　对使用时间进行限制

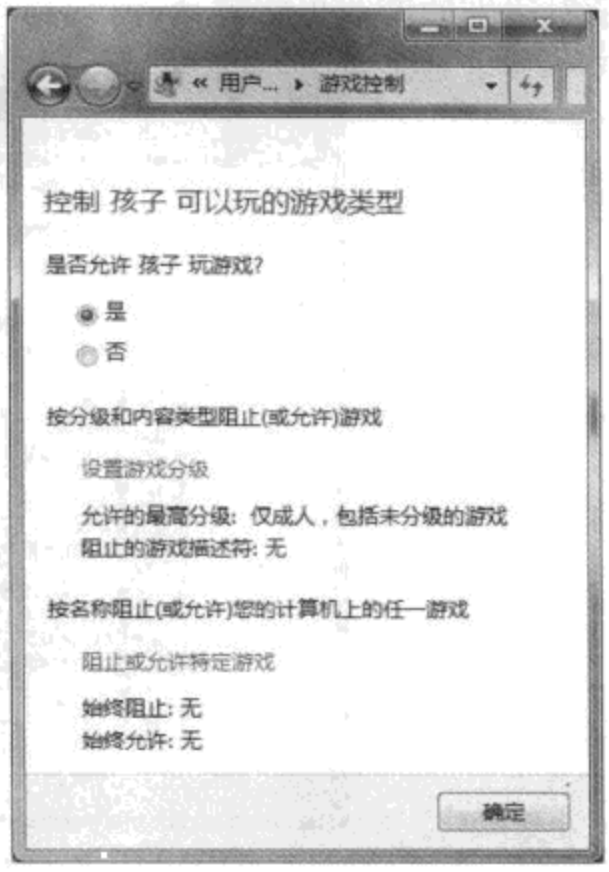


图 11-9　对可玩的游戏进行限制

首先可以通过“是否允许×××玩游戏”选项决定是否允许孩子的账户启动游戏。这里需要注意，其实游戏也是软件，只不过是各种软件中的一种，因此，该功能只能限制被 Windows 7 识别为游戏的程序（简单来说，就是可以自动出现在“游戏”浏览器中的游戏，该浏览器可以在“开始”菜单上单击“游戏”命令打开）。对于没有出现在游戏浏览器中的游戏，无法直接通过该功能进行设置，不过可以按照下文介绍的方法，将其当做一般程序来限制。

这里可以选择“否”，拒绝孩子运行任何一个识别出来的游戏；或者单击“是”，允许孩子玩游戏，但限制可以玩的游戏种类，或者限制具体的游戏。这里假设选择了“是”，然后可以通过其余选项决定允许孩子玩什么样的游戏。

在图 11-9 中单击“设置游戏分级”链接后，可以看到图 11-10 所示的界面，在这里可以通过游戏的分级信息和内容来进行限制。

首先，如果只允许孩子玩被识别出来的，并且带有分级信息的，同时级别满足设置的游戏，可以选择“阻止未分级的游戏”；如果不希望阻止没有提供分级信息的游戏，则可以选择“允许未分级的游戏”。

随后系统列出了当前选择的游戏分级系统为 ESRB，取决于所用的分级系统，这里会显示该系统对于不同游戏类别的分级信息，例如，ESRB 就是通过年龄来进行分类的，越靠前的类别，就越“干净”，而越靠后的级别中越有可能出现“不恰当”的内容。在这里只需要根据自己孩子的年龄选择即可，选择好之后，位于所选级别之前的游戏都将可以玩。例如，如果选择了“10 岁以上的所有人”级别，那么位于该级别之前的“所有人”和“儿

童”级别的游戏也将被允许。

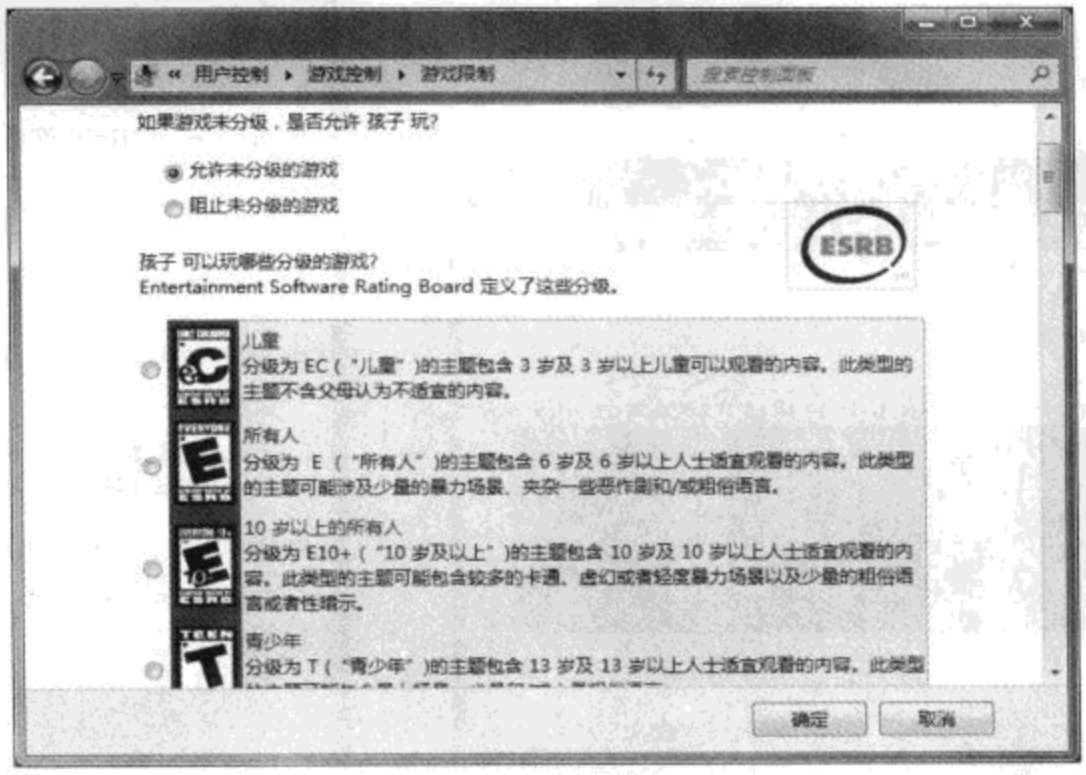


图 11-10　根据级别限制游戏

除了通过级别来限制外，还可以通过游戏的内容进行限制。将滚动条向下拖动，可以看到图 11-11 所示的界面，这里列出了游戏中可能出现的内容，对于不希望孩子玩的内容，我们只要选中相应的选项即可。

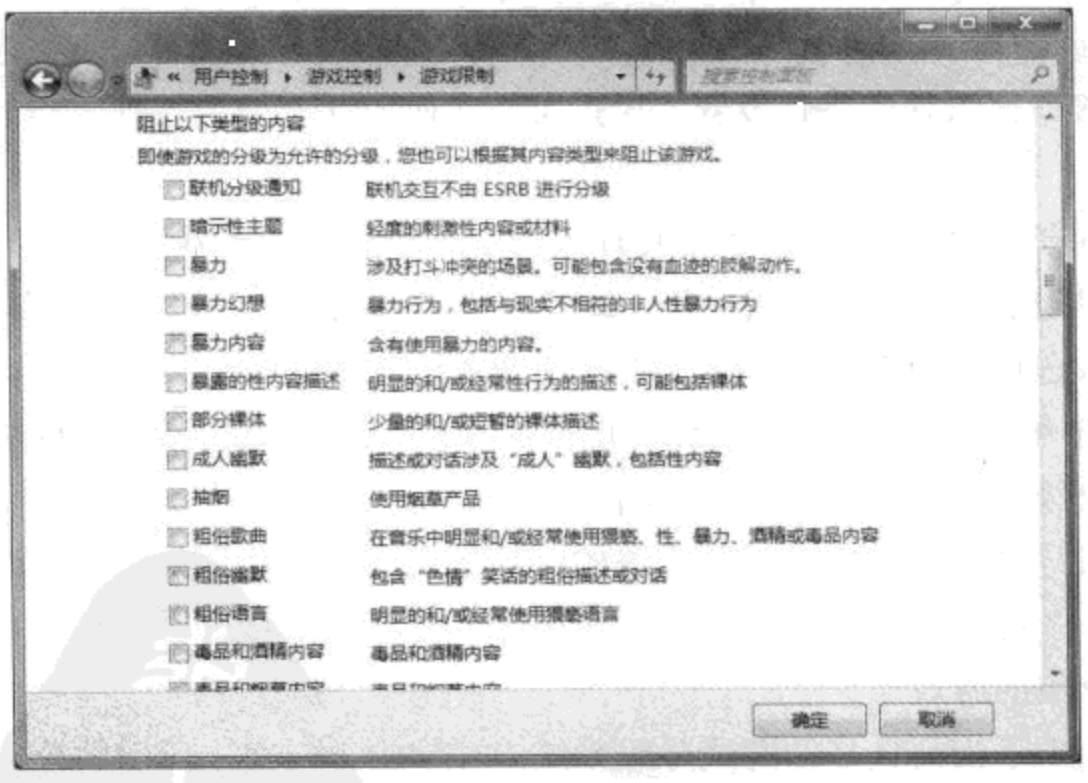


图 11-11　根据内容限制游戏

在限制游戏的时候需要注意，要想正确使用该功能，要求游戏本身必须带有必要的分级信息和内容信息，随后，Windows 才可以根据游戏提供的信息结合我们的设置判断是否允许孩子玩这个游戏。需要提醒的是，该功能只能应用到被 Windows 7 的游戏浏览器正确

识别的游戏上。

然而事实是，几乎所有的老游戏，以及大部分国内厂商发布的游戏都不包含该功能所需的信息，毕竟国内的游戏分级制度一直都没能有效地实施过。这种情况下，可以利用下文介绍的方法，将游戏当做一般软件进行限制。当然，这样也可以限制没有被 Windows 的游戏浏览器正确识别的游戏。

除了通过分级信息和内容信息来限制游戏的运行外，还可以使用黑白名单功能，而且黑白名单功能的优先级要高过分级信息和内容信息。例如，有一个游戏，如果按照分级信息来看，属于被禁止运行的，但该游戏出现在白名单中，那么这个游戏就可以被运行；同理，如果一个游戏按照分级信息来看是被允许的，但该游戏出现在黑名单中，那么这个游戏同样无法运行。

要想设置黑白名单，请单击“阻止或允许特定游戏”选项，随后可以看到图 11-12 所示的界面。

图 11-12　针对具体游戏进行限制

这里已经列出了本机上安装的，并且被 Windows 成功识别的所有游戏，每个游戏的名称下方还会显示当前的分级系统、该游戏的分级信息。如果不希望孩子运行其中某个特定的游戏，可以选择对应的“始终阻止”选项；或者也可以选择“始终允许”，这样用户忽略分级信息或者内容信息的限制，让孩子总是可以玩这个游戏。默认的“用户分级设置”则可以让系统根据游戏的分级信息和内容信息来限制。

11.2.4　设置允许和拒绝使用的程序

在图 11-5 所示的界面上单击“允许和阻止特定程序”链接后，可以看到如图 11-13 所示的界面，在这里可以针对本机安装的所有程序进行限制。

首先，如果不希望限制孩子可以运行的程序，可以选择“孩子可以使用所有程序”选项；如果希望对可以运行的程序进行限制，则需要选择“孩子只能使用允许的程序”选项。选择后者后，稍等片刻，本机安装的所有程序都会被列在下方的列表中，这些程序会按照安装目录进行分组，并带有一个复选框，我们只要选中允许运行的程序即可。

如果希望限制的程序没有被识别出来（例如，不需要安装的绿色软件），还可以单击“浏览”按钮，添加新的程序进来。

图 11-13　针对具体程序进行限制

在使用该功能的时候需要注意两个问题：

- 如果选择“孩子只能使用允许的程序”选项，那么在随后出现的程序列表中，可能会有部分程序被默认选中了。这种情况多出现在设备驱动方面，因为有些设备必须运行一个程序才能使用其功能，或者对一些选项进行设置，因此，这些程序会被系统默认选中。建议不要禁止这些程序，否则可能会对系统以及设备的正常使用造成未知的影响。
- 对于某些程序，可能需要通过不同的可执行文件实现不同的功能。例如，某些网络聊天软件，正常情况下实现文字交流功能只需要一个主文件，但如果希望通过该软件进行语音或者视频通信，或者拨打电话，则需要其他可执行文件提供支持。因此，如果希望允许孩子运行某个程序，而这个程序的同一路径下还列出了其他程序，最好同时将其他程序一同选中，以免影响到正常功能的使用。

其实，这些功能与上文介绍过的应用程序锁定策略以及软件限制策略的作用非常类似，但很明显，后两者的功能更加强大。因此，如果有必要，也可以通过应用程序锁定策略对可运行的程序进行限制。有关应用程序控制策略的详细信息，请参考 3.7 节，有关软件限

制策略的详细信息，则请参考 3.6 节。

经过上述设置，对一个账户的所有限制已经设置完毕。如果还需要针对其他账户进行设置，则需要重复上面的整个过程。

让我们看看自己的工作会有怎样的结果吧。

11.3　控制的结果

使用孩子的账户登录，并进行日常的操作，看看 Windows 7 的这些限制是否可以生效。

11.3.1　登录时间的限制

在不允许登录的时间段内，当孩子试图使用自己的账户登录时，会在欢迎屏幕上看到图 11-14 所示的错误信息。

如果是在允许的时间内登录，自然会成功，但是桌面右下角的通知区域中会显示一个家长控制图标（如图 11-15 所示）。单击该图标后，可以看到针对自己的所有家长控制选项设置。

图 11-14　非允许时间内被拒绝登录

图 11-15　证明家长控制功能生效的通知区域图标

在可用时间即将用完的时候，系统会使用气泡信息提示孩子注意，一旦可用时间用完，他的会话会被立刻断开，返回到欢迎屏幕。会话被断开后，孩子打开的文档以及运行的程序依然会在后台运行，但无法操作。只要不重启动系统，等到下一次可用时间到达后，登录系统即可继续使用。

11.3.2　网页浏览的限制

当孩子登录后，并使用浏览器访问网页时，系统就会自动将访问的地址和设置的选项进行对比。如果发现允许访问该地址，那么网页内容就会被打开，否则孩子会看到图 11-16 所示的界面。

这时候，孩子有两个选择：放弃浏览该网站，或者请求许可。如果这个网站确实是需要访问的，但是因为设置上的原因而导致被禁止，那么可以单击“亲自请求”按钮，随后系统会用一个新窗口打开登录对话框，家长在这里选择自己的 Windows Live ID 用户名，

并输入密码（输入密码时请注意保密），然后单击“预览”按钮，查看并判断该网站是否适合自己的孩子访问，随后可单击“批准”按钮，允许孩子这次以及以后对该网站的访问；或者也可以单击“拒绝”按钮，禁止孩子访问，以及禁止针对该网站再次请求许可。

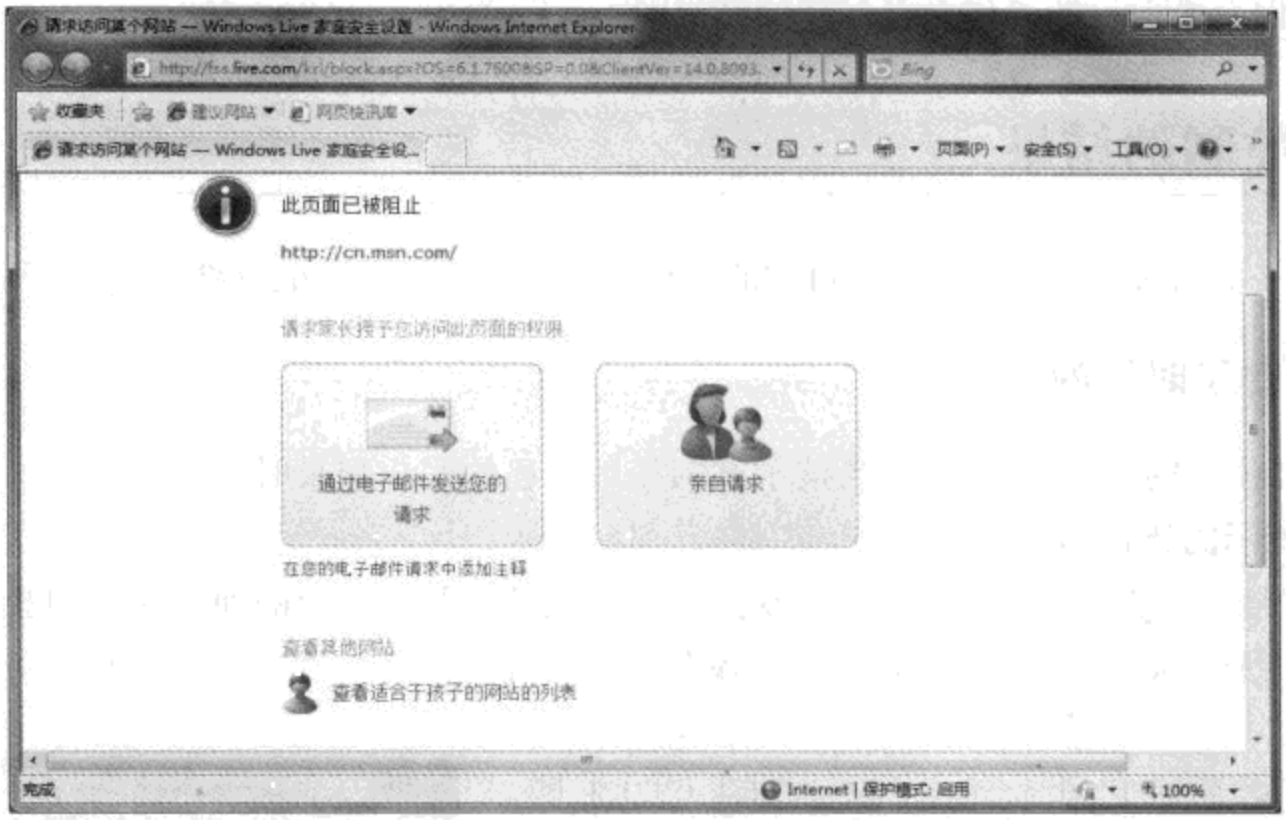


图 11-16　访问被限制的网站时的提示信息

如果家长不在身边，此时孩子也可以单击“通过电子邮件发送您的请求”按钮，随后系统会自动给家长 Windows Live ID 的注册邮箱发送一封电子邮件。邮件中会列出孩子试图访问但被拒绝的网站域名，家长需要访问这些域名，并判断是否允许孩子访问，然后在任何一台计算机上登录到 Windows Live 家庭安全设置网页（http://fss.live.com），并批准或拒绝该请求。为了使改动尽快生效，孩子可以注销自己的账户，并重新登录。

如果通过设置禁止孩子在网页上下载文件，那么当孩子试图进行下载的时候，也会看到拒绝信息。但是需要注意，对于网页中显示的图片，如果通过“另存为”的方式保存到本地，将不会受到这种下载限制。

11.3.3　运行游戏的限制

打开游戏浏览器，立刻就可以看到，对于被禁止运行的游戏，游戏的图标上会带有一个大大的“禁止”符号，同时在尝试运行这些游戏的时候也会看到详细的错误信息，如图 11-17 所示。

11.3.4　软件使用的限制

如果试图运行一个被禁止的软件，那么 Windows 将会显示图 11-18 所示的错误信息。它和游戏的不同之处在于，家长可以随时取消对一个软件的限制。

图 11-17　被家长控制功能禁止运行的游戏

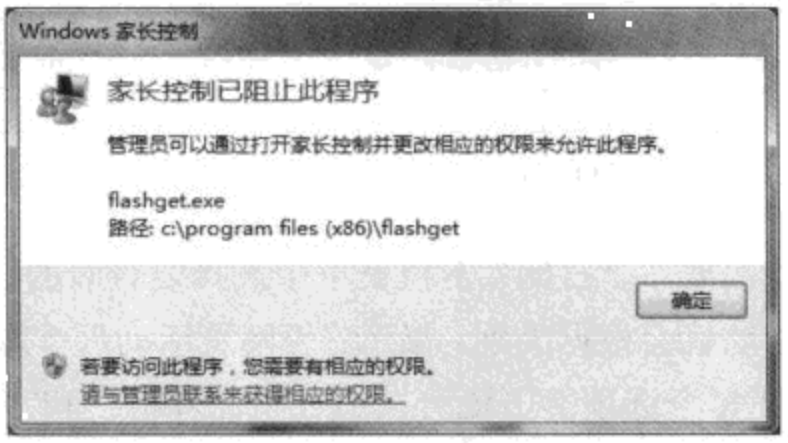


图 11-18　被禁止的软件也无法正常运行

如果孩子觉得自己确实需要使用该软件，可以单击“请与管理员联系来获得相应的权限”链接，随后会打开 UAC 的提升对话框，家长需要在这里选择自己的账户，并输入密码，然后单击“确定”按钮。如果希望孩子以后一直可以使用该软件，可以单击“始终允许”按钮，将其加入白名单；如果不希望孩子使用该软件，则可以单击“保持阻止”按钮，这样目标软件也不会运行。

与网页的限制不同，对于应用程序的限制，家长必须亲自在孩子使用的计算机上操作才可以解除限制。而网页的限制则无此要求，家长不管在何处，只要有可上网的计算机，都可解除对某一特定网站的限制，或修改 Windows Live 家庭安全功能的所有选项。

11.4　查看活动记录

通过上述操作，我们可以很容易地限制孩子对计算机的使用，然而经过一段时间后，可能还希望对孩子的使用情况进行了解。

如果需要查看孩子的活动记录，家长需要访问 Windows Live 家庭安全设置网站（http://fss.live.com）。在使用自己的 Windows Live ID 登录后，单击页面左侧的“活动报告”链接，随后即可在图 11-19 所示的界面下看到孩子在家里计算机上的所有活动报告（数据每小时更新一次，最多可保留 30 天）。

图 11-19　在网页上查看活动报告

在图 11-19 中，首先需要在“日期”下拉菜单中选择要查看的日期范围，随后单击“显示活动”按钮，所有的活动就会根据类别，显示在“网页活动”、“其他网络活动”，以及“计算机”活动选项卡下。在每个选项卡下还可以通过“计算机”和“Windows 账户”下拉菜单，选择要查看的计算机，以及这台或这些计算机上具体的 Windows 账户的活动信息。为了降低信息量，还可以选择“仅显示阻止的活动”选项。设置完显示的选项后，单击“显示活动”按钮，所有符合要求的活动都将显示出来。

在“网页活动”选项卡下，可以看到孩子的网页浏览情况，例如，在什么时间浏览过哪些网页，分别浏览过多少次。这里列出的每个域名前面还有一个小箭头，单击后即可看到该域名下所有浏览过的页面记录。

对于标注为“活动”的内容，如果发现内容实际上并不适合自己的孩子观看，还可以单击右侧的“更改设置”下拉菜单，并从中选择“仅阻止此人”或“阻止所有人”选项，这样，某一个孩子或者自己的所有孩子都将无法再次访问该网站。对于标注为“阻止”的内容，如果认为适合孩子访问，则可以单击“更改设置”下拉菜单，并从中选择“仅允许此人”或“允许所有人”，允许自己的孩子访问。

在“其他网络活动”选项卡下，列出了并非通过浏览器进行的网络活动。例如，某些软件在运行过程中需要访问网络，那么此类信息就会显示在“其他网络活动”选项卡下。作为家长，也可以根据实际情况查看这些活动，并决定是否允许或拒绝相关活动。

在“计算机活动”选项卡下，可以看到其他所有活动的相关记录（如图 11-20 所示）。

例如，登录的时间和累积时长、运行过的软件、玩过的游戏、下载过的文件等。

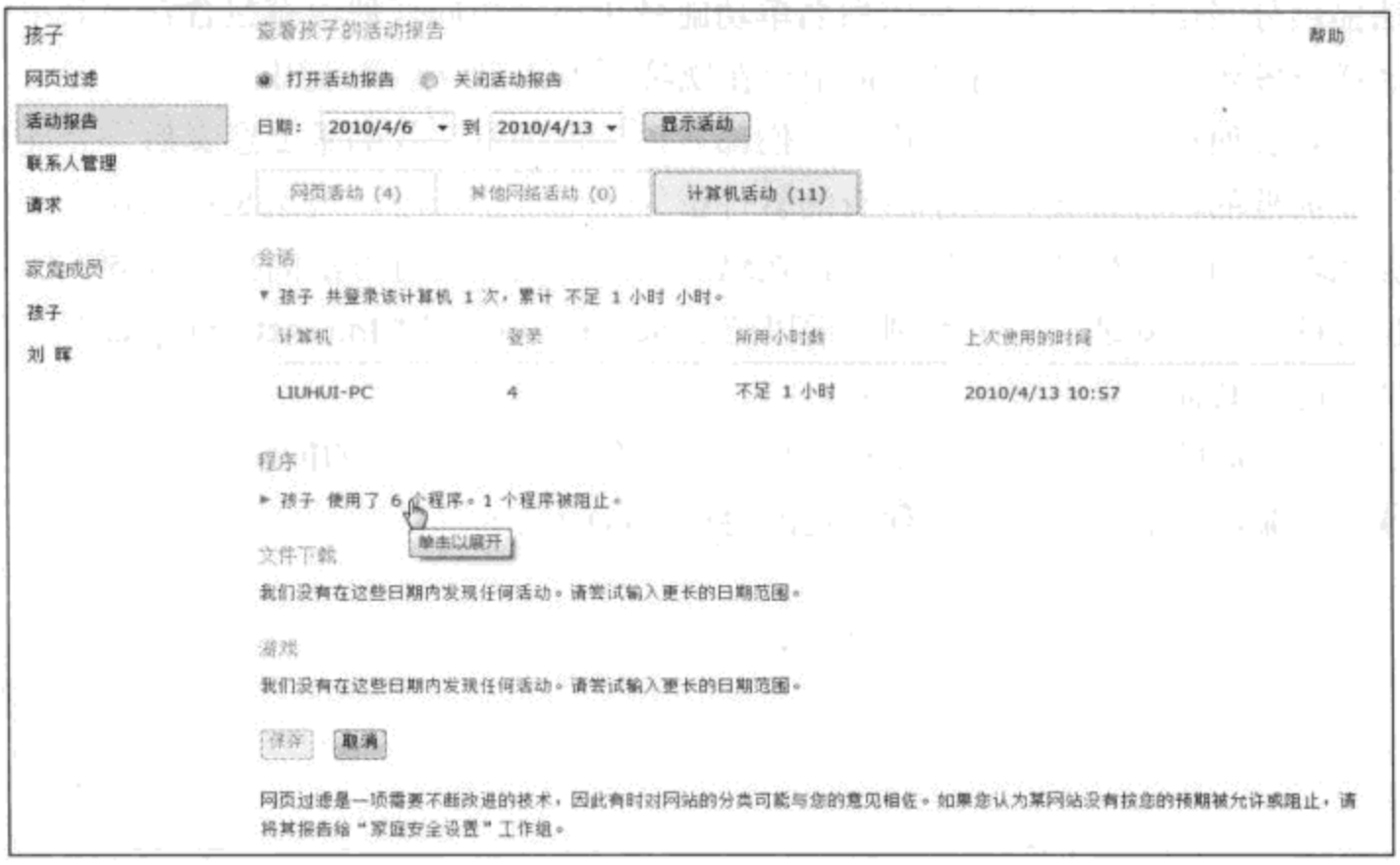


图 11-20　与网络访问无关的活动报告

注意，这里的内容只能在网页上查看，无法直接修改。要修改相关设置，必须亲自在孩子使用的计算机上进行操作。

有关家长控制功能就是这些内容。通过学习上面的内容，很多人可能已经意识到了，这确实是一个很不错的功能，并想立刻将其投入使用。然而使用后，大部分人可能会失望地发现，效果远非预料中的那么好，其原因到底是什么？是否是微软在夸大其词？其实并不是这样。

首先，保护下一代不受恶意信息的侵犯，并不是某一家公司或者某一两个人的事，而是整个社会的责任。例如，在网页内容阻止方面，家长控制功能可以通过网站提供的分级信息来判断这个网站的内容是否适合孩子观看。但这就有一个目前来说很不现实的要求：网站必须主动提交真实的分级信息。如果是一家美国公司开发的软件，这个功能在美国也许可以达到预期的目的，但在国内至少目前还是不行的，因为目前还没有什么规章制度甚至法律能够要求每个网站都提供这些信息，而且很多人并没有意识到它的重要性。同样，游戏的控制功能也面临这样的尴尬。

其次，用户具有选择权。虽然微软自家提供的程序能够被家长控制功能所制约，可并非所有的用户都愿意使用微软提供的这些程序。例如，对于孩子浏览的网页进行限制，这是通过安装在 IE 中的加载项实现的，很明显，对于非 IE 浏览器用户，将无法受到该功能的任何限制。可并不是所有的人都愿意使用微软的 Internet Explorer 浏览器，而且至少在目前来看，其他非微软的同类软件都还没有这样的功能。

当然，要解决这些问题也并非不可能。例如，对于网络访问的限制，虽然目前很多网站无法提供分级信息，但可以使用白名单功能禁止孩子访问任何没有包含在白名单中的站点。这样在操作上虽然比较麻烦，但至少在现阶段一样可以起到作用。

至于对其他程序的监控，也许当人们都意识到保护下一代的重要意义后，会促成一个类似行业标准的内容发布，几乎所有的软件都能遵循这个标准，被家长控制功能或者其他具有类似功能的软件所监管和控制。但在这之前，我们还是有办法间接实现同样的目的，如果担心孩子自己安装一个其他浏览器以绕过家长控制功能对 Internet Explorer 的监管，可设置禁止运行其他浏览器软件的安装。

最后，也是最重要的一点：技术并不是万能的。如果做家长的能够多关心、鼓励孩子，多和孩子交流，他们又怎么会愿意总是沉迷在虚拟的电子世界中？

CHAPTER

12

第 12 章　BitLocker 与 BitLocker To Go

BitLocker 是从 Windows Vista 开始新增的一项功能，并且可用于 Windows 7 系统，但只能用于 Windows 7 企业版/旗舰版。该功能可以将本地硬盘分区进行加密，防止被脱机攻击和数据泄密。

BitLocker To Go 则是 Windows 7 的新功能，该功能可对可移动存储设备进行加密，并可防范数据泄密。

在继续进行下文之前，有必要对脱机攻击进行简单的介绍。在本书开头几章已经介绍过，为了保证系统的安全，必须给自己的账户创建一个强密码，并且可以通过 NTFS 权限和 EFS 加密对重要的数据进行保护，限制访问。然而这样就可以做到万无一失吗？如果给自己的账户添加了强密码，真的就能保证别人无法使用自己的账户登录？其实未必。

本书第 1 章介绍了一种用于破解单机环境 Windows 账户密码的软件，这个软件是免费的。因此，在使用上可能还存在一定的难度，所有的操作都需要在英文的字符环境下进行。但实际上，类似的软件还有很多，并且其中一些收费软件的易用性非常好，Windows 账户密码的破解也变成了一种非常简单的工作。

很多人可能都听说过 ERD Commander 之类的软件，这种软件可以创建一个光盘镜像文件，将其刻录到光盘上之后，可以用来引导计算机启动。这种软件的强大之处在于，可以将计算机引导进入一种 Windows PE 环境(可以理解为运行在光盘上的 Windows 系统)，而这个环境中有一些程序，可以在硬盘上原先安装的 Windows 没有启动，而自己也不知道管理员账户密码的情况下看到这个 Windows 的注册表内容，并在不知道现有密码的前提下修改任何一个本地账户的密码，当然，对于获取文件的 NTFS 访问权限、EFS 加密的密钥，甚至网络银行的安全证书等信息更是小菜一碟。这种攻击都是在 Windows 没有运行的情况下进行的，因此，被叫做“脱机攻击”。

那么，这是否就意味着 Windows 的安全性很差呢？其实也不然。因为进行脱机攻击的时候，被攻击的 Windows 并没有运行，因此，Windows 的各种安全保护机制也无法生效，进而造成了被攻击的可能。其实不仅仅是 Windows 系统，很长一段时间里，任何操作系统都无法有效地避免这种脱机攻击。至于从物理层面的攻击，例如，恶意拔掉服务器电源导致服务中断，或者损坏硬件造成数据丢失，更是无法仅依靠操作系统就能避免。所以说，

实现系统安全和数据安全的一个大前提就是首先要保证计算机在物理上的安全，不让攻击者从物理上接触到计算机。

好在 Windows 7 中的 BitLocker 功能至少可以保护整个 Windows 本身不被脱机攻击。简单来说，BitLocker 会将 Windows 的安装分区进行加密，并将密钥保存在硬盘之外的地方。这样，要想启动 Windows，就必须先提供密钥，随后引导程序才会使用提供的密钥解密系统文件，并加载和运行 Windows。

> **注意** 在初始版本的 Windows Vista 中，BitLocker 功能只能加密操作系统所在的分区，无法加密其他分区。不过在 Windows Vista Service Pack 1 以及 Windows 7 中，BitLocker 功能经过改进，已经可以对任何本地硬盘分区进行加密。

BitLocker 主要有两种工作模式：TPM 模式和 U 盘模式（为了实现更高程度的安全，还可以同时启用这两种模式）。

- 要使用 TPM 模式，要求计算机中必须带有不低于 1.2 版 TPM 芯片，这种芯片是通过硬件方式提供的，一般只出现在对安全性要求较高的商用计算机或者工作站上，家用计算机或者普通的商用计算机上通常不会提供。要想知道计算机上是否有 TPM 芯片，需要运行“devmgmt.msc”打开设备管理器，然后查看设备管理器中是否存在一个叫做“安全设备”的节点，该节点下是否有“受信任的平台模块”这类设备，并确定其版本即可。
- 如果要使用 U 盘模式，只需要计算机上有 USB 接口，计算机的 BIOS 支持在开机的时候访问 USB 设备（基本上，能够流畅运行 Windows 7 的计算机都应该具备这样的功能），并且能提供一个专用的 U 盘即可（U 盘只是用于保存密钥文件，容量可以不用太大，但是一定要求质量要好）。使用 U 盘模式后，用于解密系统盘的密钥文件会被保存在 U 盘上，每次重启动系统的时候，必须在开机之前将 U 盘连接到计算机上。

如果能够从硬件上满足上述要求，那么就可以体验一下 BitLocker 的强大之处了。但是在实际操作之前，还请先检查一下硬盘分区是否满足 BitLocker 的要求。

12.1 使用 BitLocker 的前提条件

通常情况下，我们可能习惯这样给硬盘分区：首先，在第一块硬盘上划分一个活动主分区，用于安装 Windows，这个分区是系统盘；其次，对于剩下的空间继续划分更多的主分区，或者创建一个扩展分区，然后在上面创建逻辑驱动器。简单来说，我们已经习惯于让第一块硬盘的第一个分区成为系统盘，并在上面安装 Windows。

例如，图 12-1 所示的界面就是在一台安装 Windows 7 的计算机上运行“diskmgmt.msc”

后看到的硬盘分区情况。

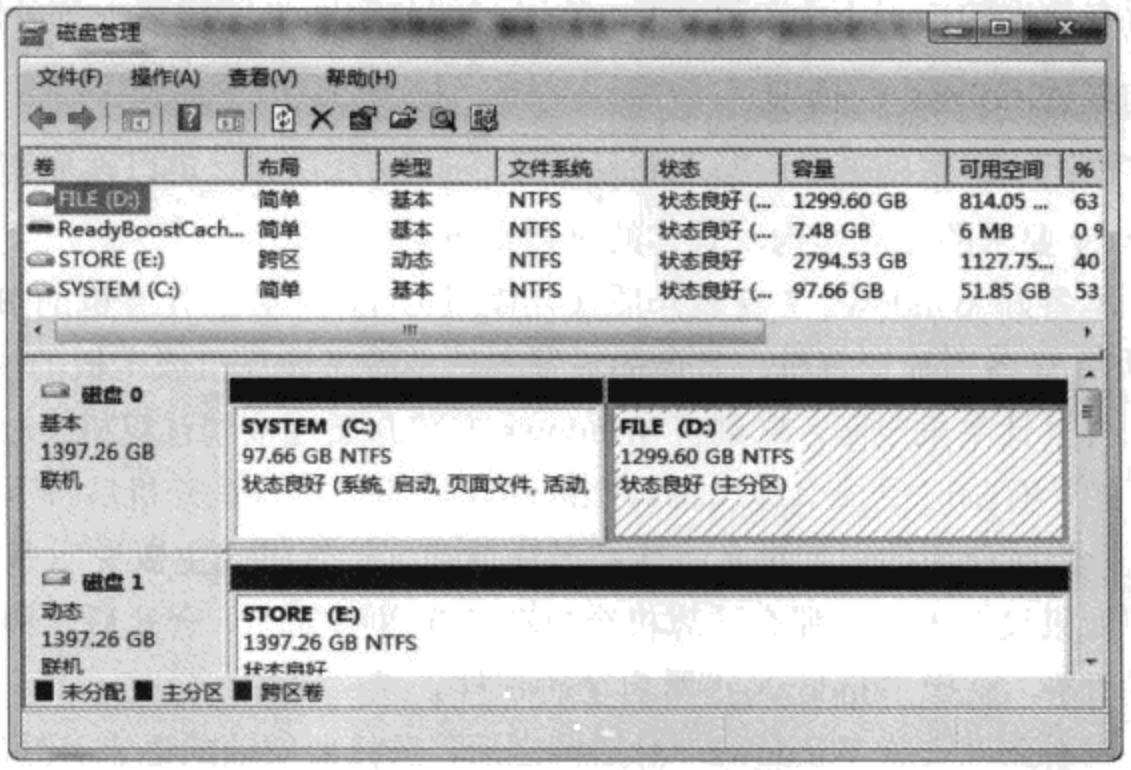


图 12-1　很多人所惯用的磁盘分区方案

因为印刷的关系，大家在图上看不出通过颜色区分的不同类型的分区，不过大家完全可以在自己的计算机上打开磁盘管理控制台，观察自己硬盘的分区情况。请注意图 12-1 中的“磁盘 0”，该磁盘上有两个分区，对应的盘符分别是“C”和“D”，其中的“C”就是第一块硬盘上的第一个分区，属于系统盘，而且是活动的。但问题在于，如果除了系统盘外，硬盘上不存在其他活动分区，是无法直接针对系统盘启用 BitLocker 的（无论是 TPM 模式还是 U 盘模式）。为什么？

在前面已经说了，BitLocker 功能实际上就是将操作系统所在的硬盘分区进行加密，在启动系统的时候，必须提供解密的密钥来解密原本被加密的文件，这样才能启动操作系统。但这就有一个问题，用于解密的密钥可以保存在 TPM 芯片或者 U 盘中，但是解密程序（其实除了解密程序，还有很多文件的位置需要关注，这里不准备详细说明）应该放在哪里呢？难道就放在系统盘中吗？可是系统盘已经被加密了，这就导致了一种很矛盾的状态：因为用于解密的程序被加密了，因此，无法运行，导致无法解密文件。

如果要顺利地使用 BitLocker 功能，硬盘上必须至少有两个活动分区（对于 x86 架构的 PC 机，最多可以有 4 个活动分区），除了系统盘外，额外的活动分区必须保持未加密状态，且必须是 NTFS 文件系统，同时，可用空间不能少于 100 MB（很明显，单纯的解密程序以及引导系统所需的文件不会有这么大，但微软要求这个分区不小于 100 MB，估计是为了保存解密过程中产生的临时文件）。

如果还未安装 Windows 7，并且打算安装好系统之后使用 BitLocker 功能，那么在安装的时候可直接将分区准备好。

如果你已经安装了 Windows 7，并且在打算使用 BitLocker 的时候才看到上述内容，而

硬盘分区已经按照传统的方式划分好了，那么也不用担心。通过一些方法，可以在不破坏现有系统和所有数据的前提下为 BitLocker 腾出一部分空间来创建第一个分区。

1. 未安装 Windows 的情况

如果正打算在一块新硬盘上安装 Windows 7 企业版/旗舰版，可以在安装的过程中创建出符合 BitLocker 要求的分区结构。具体的过程如下：

STEP 01 准备好 Windows 7 安装介质（光盘或 U 盘），并在计算机的 BIOS 设置中设定通过光盘/USB 设备引导计算机（具体的设置方法请参考计算机或主板的说明书）。

STEP 02 打开计算机电源，立刻将 Windows 安装介质连接到计算机（对于较新的计算机或主板，可能带有临时更换引导设备顺序的功能，通常可以在开机后按下键盘上的某个按键，然后选择临时使用的引导设备，详细做法请阅读计算机或主板说明书）。

STEP 03 如果设置无误，那么计算机会自动从光盘引导，一会儿后，屏幕上就会出现一个绿色的滚动条，就像 Windows 正常启动时那样。

STEP 04 当看到“安装 Windows”对话框之后，选择要安装的语言、时间、货币格式，以及键盘和输入方法，设置好之后单击“下一步”按钮。

STEP 05 继续单击“下一步”按钮，直到看到图 12-2 所示的选择安装位置的界面。

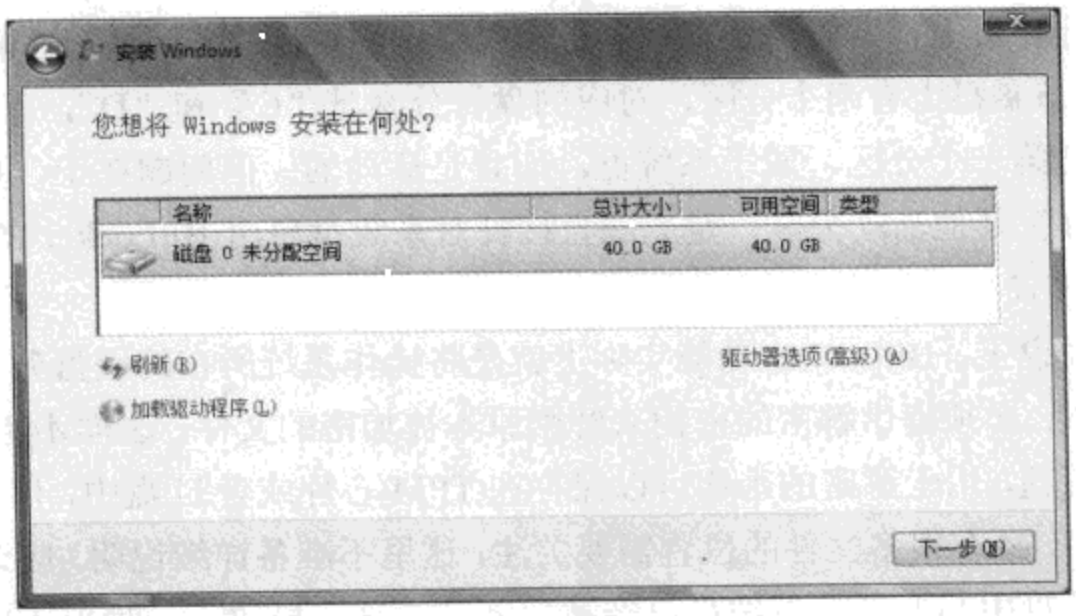


图 12-2　选择 Windows 的安装位置

STEP 06 无论是使用了尚未创建分区的新硬盘，还是已经创建了分区的老硬盘，在这里需要注意，一定要选择足够大小的“未分配空间”作为安装位置。

- 如果这是一块新硬盘，尚未创建分区，但打算给系统盘分配 50 GB 空间，其他空间创建三个分区。首先需要根据情况，创建一个 50 GB 的系统盘，并创建其余三个分区，将硬盘总空间全部分配完毕。随后将 50 GB 的系统盘删除，产生 50 GB 的“未分配空间”作为安装位置。
- 如果这是一块老硬盘，已经创建了分区，并且用于安装 Windows 的第一个分区已经存在，此时可以直接将该分区删除，产生“未分配空间”，并将其作为安装位置。

这样做的唯一目的就是：选择“未分配空间”作为 Windows 的安装位置，而不要选择任何现有的分区。这样安装程序会自动创建两个分区，即一个 100 MB 的隐藏分区，用于保存不能被加密的 Windows 引导文件；其余空间创建“C 盘”，用于保存 Windows 中所有的系统文件。

经过上述设置并安装 Windows 7 后，就可以随时启用 BitLocker 功能。

2．已安装 Windows 的情况

如果已经安装了 Windows，并在打算启用 BitLocker 的时候才发现系统被安装到磁盘 0 分区 1 上，也不用担心。只要分区 1 的可用空间够用，完全可以将其中一部分空间拆借出来，创建一个新的磁盘 0 分区 1。

要想在保留现有数据的前提下给原本安装了 Windows 的“磁盘 0 分区 1”前面新建一个分区，可以由 Windows 7 的 BitLocker 功能自动帮我们完成，甚至不需要进行任何额外的操作。因为在打算对系统盘应用 BitLocker 加密之前，系统会对硬盘进行初始化，如果发现硬盘分区布局不符合要求，则可以自动进行调整。我们只需要在要求的时候重启动系统，即可完成分区的调整工作。

同时，为了确认准备工作的完成，在重启动系统后，可以再次运行“diskmgmt.msc”，打开磁盘管理工具，随后可以看到图 12-3 所示的界面。请和图 12-1 显示的内容进行对比，以了解该工具具体对硬盘进行了哪些操作，重点注意是否出现了大小为 100 MB 的“系统保留”分区。

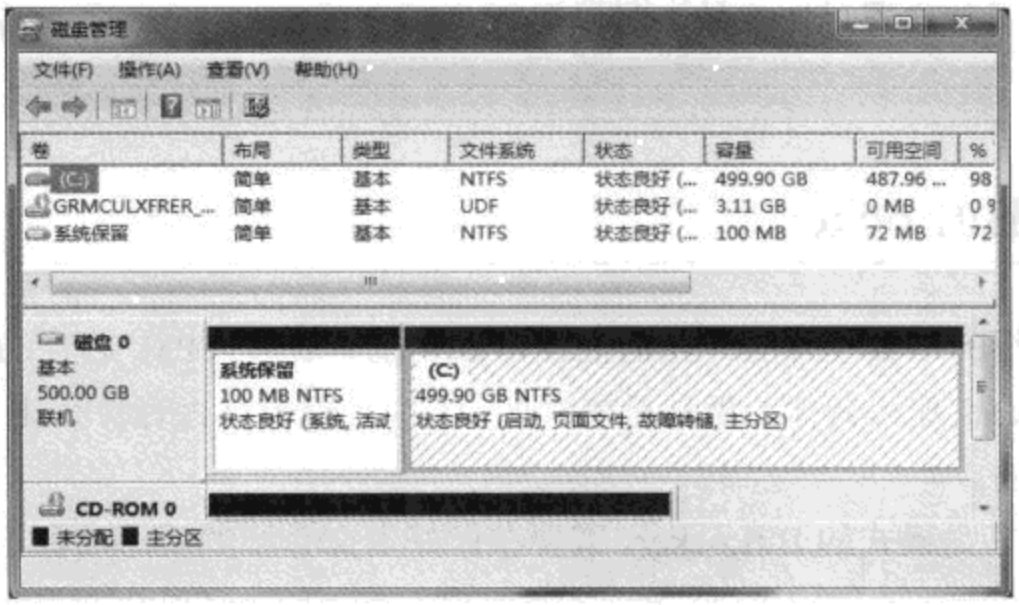


图 12-3　符合要求的分区布局

另外，由于在默认情况下，系统中只能使用 TPM 模式的 BitLocker，若要使用 U 盘模式，还必须配置组策略将其启用。具体做法如下：

STEP 01 运行“gpedit.msc”，打开组策略编辑器，从编辑器窗口左侧的控制台树形图中定位到“计算机配置”→“管理模板”→“Windows 组件”→“BitLocker 驱动器加密”→“操作系统驱动器”。

STEP 02 在右侧的控制台窗口中找到并双击打开“启动时需要附加身份验证”策略，选择“已启用”（如图 12-4 所示）。

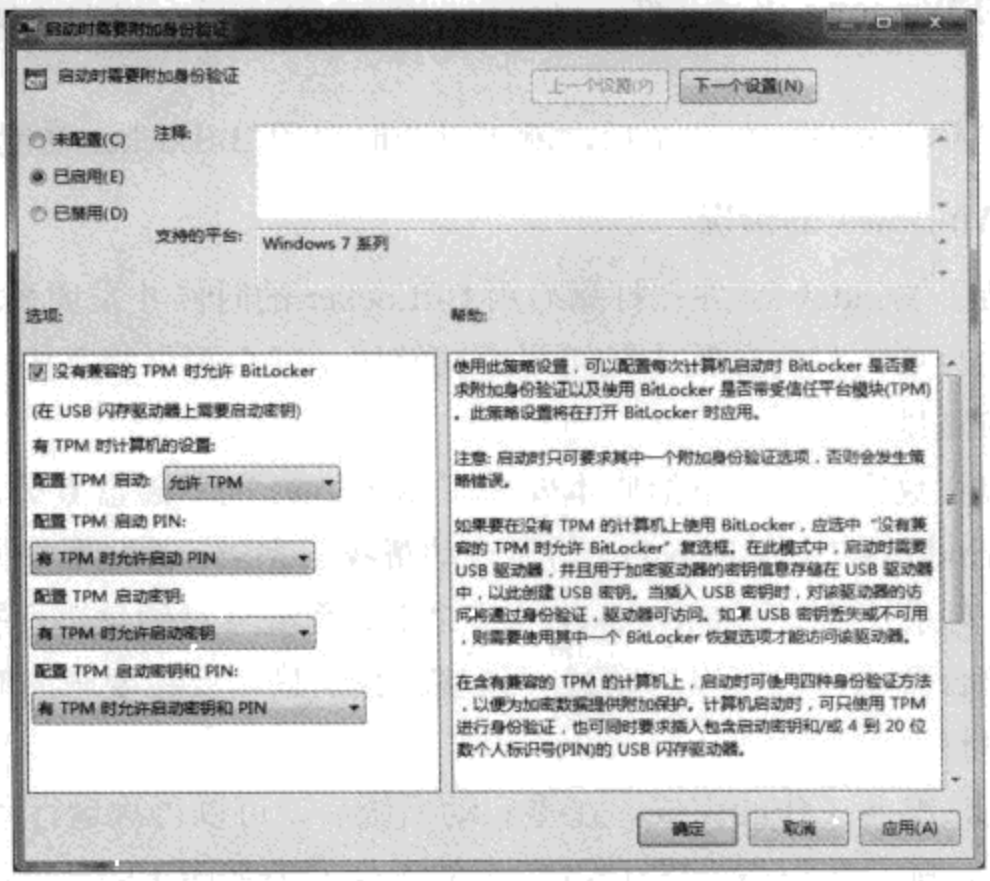


图 12-4　根据实际需要选择不同的配置方式

STEP 03 单击“确定”按钮保存设置，这样我们就在本机启用了 U 盘模式的 BitLocker。

STEP 04 为了使设置尽快生效，可以运行“gpupdate.exe /force”命令强制本机刷新组策略配置。

12.2　启用 BitLocker

经过上文介绍的步骤设置后，我们已经可以在没有安装 TPM 芯片的计算机上使用 U 盘模式的 BitLocker。那么具体的做法是怎样的，整个过程中是否有什么注意事项需要了解，这是本节要介绍的。

如果要启用 U 盘模式的 BitLocker，需要在做好上文介绍的所有准备工作之后进行下列操作：

STEP 01 打开“控制面板”，依次单击“安全”→“BitLocker 驱动器加密”，我们可以看到图 12-5 所示的界面。

STEP 02 请注意右侧显示的内容，在“BitLocker 驱动器加密”选项下会列出所有可加密的本地硬盘分区，而“BitLocker 驱动器加密 - BitLocker To Go”选项下，则会列出所有可被加密的可移动存储设备分区。对于安装了 Windows 的硬盘分区或其他本地硬盘分区，单击“启用 BitLocker”链接。

STEP 03 随后可以看到图 12-6 所示的界面，在这里需要选择 BitLocker 的工作方式。如果没有 TPM 芯片，则只能选择最后一个选项，这样以后每次启动系统的时候都必须提供保存了密钥的 U 盘，不过系统启动后就不再需要了。如果有硬件的 TPM 芯片，则可以选择前两个选项。请根据实际需要进行选择。如果选择“使用没有附加密钥的 BitLocker”，则通过 TPM 芯片即可进行解密，这样的硬盘连接到其他计算机上将无法读取数据；如果选择“每次启动时要求 PIN”，也需要使用 TPM，但同时要求启动系统时输入一个指定的密码（并不是 Windows 账户的密码），这样可以做到双重保险。由于没有 TPM，打算使用 U 盘模式，因此，请直接单击“每次启动时都要求启动密钥”。

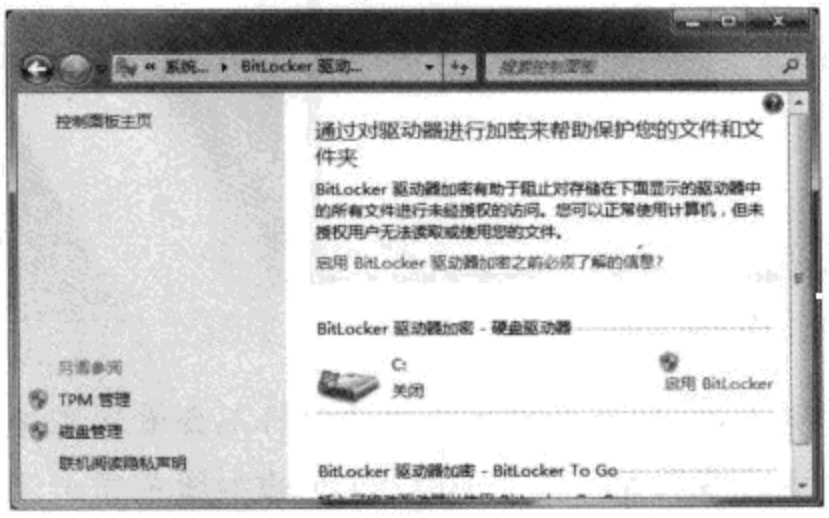


图 12-5　对特定的卷进行加密

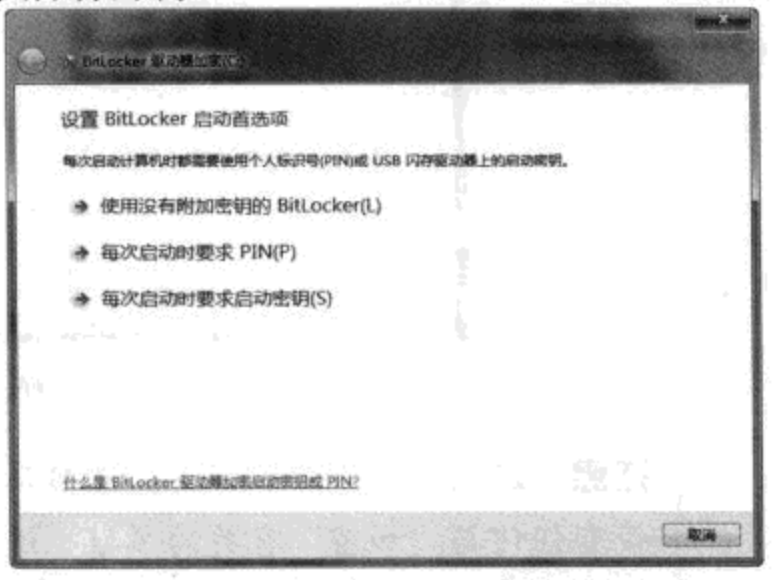


图 12-6　选择 BitLocker 的工作方式

STEP 04 将准备好的 U 盘连接到计算机，待程序界面上显示了这个 U 盘后，单击将其选中，然后单击“保存”按钮。这样用于解密被 BitLocker 加密的分区所需的密钥就会被保存在所选的 U 盘上。

STEP 05 随后可以看到图 12-7 所示的界面，在这里需要决定恢复密码的处理方式。注意，在平时的使用过程中，并不需要提供恢复密码，只要提供前一步操作中指定的 U 盘即可。而恢复密码是在 U 盘不可用（例如，丢失或者损坏）的情况下使用的。因此，建议将其妥善处理，例如，如果本机安装了打印机，可以将恢复密码打印在纸上，并将这张纸保存在安全的地方。同时，建议保留恢复密码的多个副本，例如多次打印，然后将打印的密码分别保存在不同的安全位置，或者保存在其他的 U 盘上（最好不要将恢复密码和启动密码保存在同一个 U 盘上）。

STEP 06 保管好恢复密码后，单击“下一步”按钮，随后程序会询问是否进行系统检测，以便确认可以在开机后读取启动密钥或者恢复密码。建议单击“继续”按钮，进行检测（注意：在整个过程中，最先使用的保存了启动密钥的 U 盘一定不能拔下来，如果需要将恢复密码保存在其他 U 盘上，请将第二块 U 盘连接到计算机的其他 USB 接口上）。

STEP 07 检测工作需要重启动系统，如果经检测确认无误，系统会自动开始进行加密。加密操作需要一定的时间，主要取决于系统盘的大小以及计算机的硬件速度。不过，好在这个操作只需要进行一次，而且在日后的使用过程中，系统的运行速度并不会有太大的降

低，因此，可以放心使用。加密完成后，单击“完成”按钮即可。

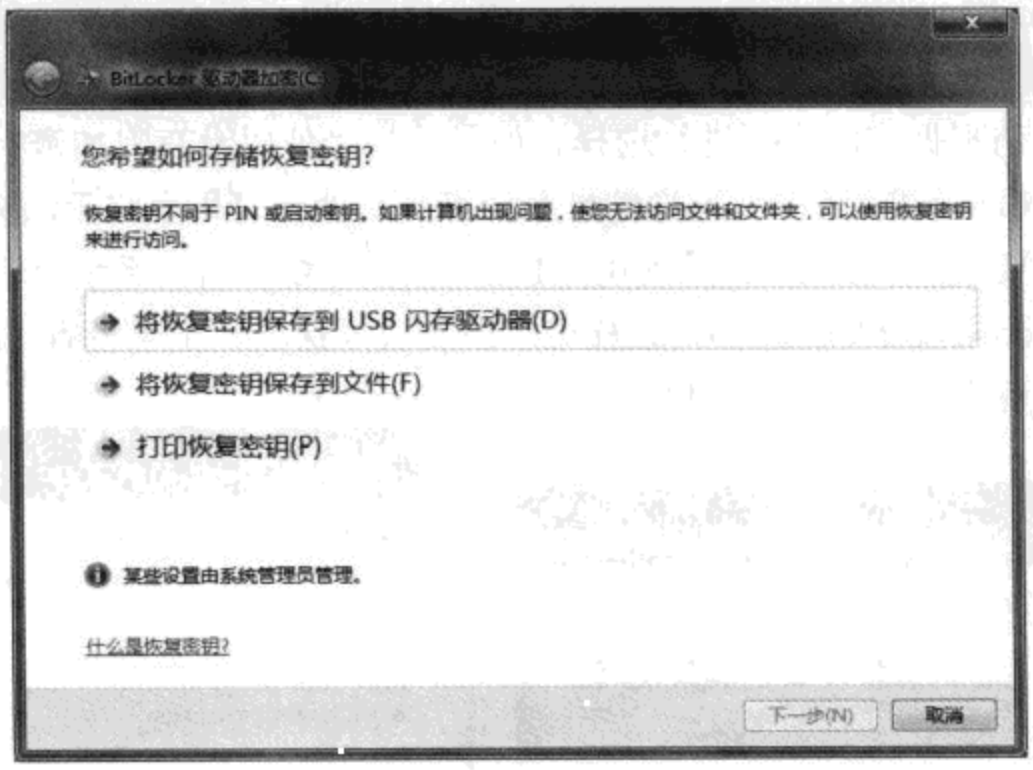


图 12-7　选择恢复密钥的处理方式

注意　应用 BitLocker 加密，并启动 Windows 后，查看系统文件时将不会看到文件带有任何与“加密”有关的属性，这属于正常现象。因为 BitLocker 的加密是在系统底层从文件系统上实现的，而在用户看来，启动好的系统文件并没有被加密。但如果换个角度来看，例如，一台计算机上安装了两个系统，或者将装有系统的硬盘拆掉，连接到其他计算机上，在试图访问应用了 BitLocker 的系统所在的分区时，我们会收到拒绝访问的信息，拒绝的原因是目标分区没有被格式化。这都属于正常现象，而且也证明了 BitLocker 正在保护我们操作系统的安全（设想一下，连访问分区都无法实现，又如何进行脱机攻击？）。

另外，保存了启动密钥的 U 盘直接在 Windows 资源管理器下查看的时候，也完全看不到其中保存的密钥文件。这也是为了安全，同时建议这个 U 盘只用于保存 BitLocker 的启动密钥，而不要用做其他用途，这主要是为了尽量避免 U 盘因为各种原因（例如病毒感染或者频繁写入损坏）造成系统无法访问。注意，密钥盘只是在启动系统的时候需要，只要系统启动好就可以将其拔出，并妥善保管起来。操作系统在正常运行过程中并不需要我们反复提供密钥盘。

最后一点，在加密过程中，系统盘的可用磁盘空间将会急剧减少。这属于正常情况，因为这个过程中会产生大量的临时文件。加密完成后，这些文件会被自动删除，同时可用空间的数量会恢复正常。在解密被加密的系统盘时也会遇到类似的情况。

在应用了 U 盘模式的 BitLocker 后，每次启动系统前都必须将保存了启动密钥的 U 盘连接到计算机，如果无法提供 U 盘，将会看到图 12-8 所示的界面。

图 12-8　无法提供解密所需的 U 盘时使用恢复密钥来恢复

这就要求我们必须将保存了启动密钥的 U 盘连接到计算机后重启动，才能完成 Windows 的启动和加载过程。如果因为某些原因，例如，保存了启动密钥的 U 盘损坏或者丢失，只要还保留有启用 BitLocker 时创建的恢复密码，则可以在这个界面上按下回车键进行恢复（详细的恢复方法请参考下一节内容）。

12.3　BitLocker 的灾难恢复

如果在启用了 BitLocker 加密后，因为各种原因导致系统无法启动，例如，保存了启动密钥的 U 盘丢失或者损坏，那么只要还保留着之前的恢复密码，也可以将其恢复出来。经过恢复操作，可以重新创建一个启动密钥盘，同时，之前创建的密钥盘将会被自动作废。这样就算别人窃取了密钥盘，只要能及时发现，并及时执行恢复程序，创建新的密钥盘，那么，获得老密钥盘的人也无法访问我们的系统。

如果需要进行恢复，请在系统启动时要求提供密钥盘的界面上直接按下回车键，随后将看到类似下面的界面：

```
Windows BitLocker 驱动器加密密码项
请输入此驱动器的恢复密码

_ _ _ _ _ _  _ _ _ _ _ _  _ _ _ _ _ _  _ _ _ _ _ _
_ _ _ _ _ _  _ _ _ _ _ _  _ _ _ _ _ _  _ _ _ _ _ _
驱动器标签：PC   Windows 7 2009/11/8
密码 ID:
590CBF12-E0CE-4B45-A6FA-EAE1031A9D39
请用功能键 F1 到 F9 代表数字 1 - 9。使用 F10 键代表 0。
使用 Tab、Shift-Tab、Home、End 和箭头键来移动光标。
可以使用向上键和向下键这两个键来修改已输入的数字。
ENTER=继续          Esc=退出
```

这时请找出当初启用 BitLocker 时创建的启动密码，例如，可能将密码打印在纸上，或者保存在其他 U 盘或者网络共享文件夹中。

在恢复页面上用键盘上的“F1”～“F9”键代表 1～9 这 9 个数字，用“F10”键代表数字 0，输入正确的恢复密码。只要密码输入正确，输入完最后一位后，整个屏幕会黑屏，同时硬盘灯开始频繁闪烁。这时候不用着急，等待片刻后，即可看到 Windows 7 的登录界面。

当然，如果在创建恢复密码的时候选择保存在 U 盘上，这时候直接提供保存了恢复密码的 U 盘也可以实现同样的结果，而且更快捷。不过有一点需要注意，如果使用恢复密码启动了系统，那么建议重新创建启动密钥盘，否则每次启动系统的时候都需要提供恢复密码，不是很方便。创建的方法如下：

STEP 01 使用恢复密码启动系统，并使用管理员账户登录后，在“控制面板”中依次打开“安全”→“BitLocker 驱动器加密”。

STEP 02 对于被加密的分区，单击对应的“管理 BitLocker 密钥”链接，随后将打开密钥管理界面。

STEP 03 如果因为丢失了启动密钥而需要重新创建密钥盘，可以单击“复制启动密钥”按钮，并根据屏幕上的提示提供一个空白的 U 盘，完成后续操作。

STEP 04 如果希望在更多的地方保存恢复密码，则可以单击“再次保存或打印恢复密钥”按钮，并继续后面的操作。

注意

①对于启动密钥，实际上是一个扩展名为“.fek”的具有隐藏属性的文件，该文件会被放置在启动密钥盘的根目录下。因此，完全可以通过手工复制文件的方式将该文件放在更多的 U 盘上，或者放在其他计算机的硬盘上，只有在需要的时候才复制到 U 盘的根目录下，作为备份的密钥盘使用。要想在 Windows 资源管理器中看到这个文件，需要对 Windows 资源管理器进行一些设置：打开“计算机”窗口，按下键盘上的“Alt”键显示菜单栏，依次单击“工具”→“文件夹选项”→“查看”，在随后打开的“查看”选项卡中选中“显示隐藏文件”选项，并反选“隐藏受保护的操作系统文件（推荐）”选项即可。通过这样的方法，我们可以手工创建出多个可以同时使用的启动密钥盘。但一定要注意，每个启动密钥盘都必须妥善保管。

②如果已经丢失了启动密钥，而使用本节介绍的方法通过恢复密码启动了系统，这时候可以按照上文介绍的方法让系统为我们重新创建密钥盘。这个过程和手工复制文件“备份”密钥盘的结果是一样的，只不过由 Windows 代替我们完成而已。注意，对于因为启动密钥盘损坏导致的启动密钥丢失，可以借助这种方法恢复；如果是启动密钥盘失窃导致系统无法启动，那么在使用恢复密码启动系统之后，最好能够更新启动密钥，否则得到原先启动密钥盘的人将可以使用这个密钥盘访问我们的系统。在 Windows 7 中，目前无法主动更新启动密钥，必须首先解密对系统盘的加密，并禁用 BitLocker，然后重新启用，并加密系统盘。具体方法会在下文介绍。

12.4　BitLocker 的关闭

如果在启用 BitLocker 后因为某种原因不想继续使用这一功能，可以考虑将其关闭。在 Windows 7 中，有两种方法可以关闭 BitLocker：禁用 BitLocker 或者解密系统盘。

简单来说，禁用 BitLocker 是一种临时性的措施。在禁用 BitLocker 后，系统盘仍然处于被 BitLocker 加密的状态下，不过系统会自动生成一个包含了启动密钥的临时文件放在本地硬盘上。也就是说，系统启动的时候，将不再需要提供启动密钥盘，而是直接借助硬盘上保存的密钥文件来解密。这种方法适合需要临时禁用 BitLocker 的情况。例如，我们可能需要更新计算机的 BIOS，或者更改启动文件（例如，在原有 Windows 7 的基础上安装其他 Windows 系统，形成多系统环境）。这种情况下，为了确保操作可以顺利进行，就必须暂时性禁用 BitLocker。当操作完成后，还可以重新启用 BitLocker，这样硬盘上保存的临时密钥文件将会被自动删除，而我们可以使用之前创建的启动密钥盘和恢复密码对 BitLocker 功能进行操作。**在禁用模式下，系统依然可以受到 BitLocker 的部分保护**。

至于解密系统盘，则是一种比较彻底的方式。在这种方式下，启动密钥盘会被彻底禁用，而如果是 TPM 模式，则 TPM 芯片中保存的信息也会被撤销，同时系统盘的所有文件会被解密。因此，解密系统盘适合不打算继续使用这个功能的时候使用。**解密系统盘后，系统将完全不会受到 BitLocker 的保护**。

12.4.1　禁用 BitLocker

如果需要禁用 BitLocker，可以这样操作：

STEP 01　使用管理员账户登录 Windows，打开“控制面板”。

STEP 02　依次进入到“安全”→“BitLocker 驱动器加密”，单击“挂起保护”链接，随后将看到询问并确认的对话框。

STEP 03　单击“是”按钮，确认暂停保护。

随后如果需要重新启用 BitLocker，只需要单击桌面右下角系统通知区域的 BitLocker 图标，并在出现的窗口中单击“恢复保护”链接，BitLocker 立刻就会被重新启用。

12.4.2　解密系统盘

如果不再需要 BitLocker 功能，可以将其彻底禁用，并将系统盘解密。具体做法如下：

STEP 01　使用管理员账户登录 Windows 7，打开“控制面板”。

STEP 02　依次进入到“安全”→“BitLocker 驱动器加密”，单击“关闭 BitLocker”链接。

STEP 03　单击“解密驱动器”按钮，系统会自动将所有的启动密钥和恢复密码作废，并开始解密系统盘。

注意，解密操作和加密操作几乎要使用同样长的时间，而且该操作只可以暂停，无法被取消。

12.5 其他有关 BitLocker 的注意事项

BitLocker 能够做到的其实还有很多，例如，TPM 模式的使用，或者混合模式的使用等。如果需要更高程度的安全性，我们还可以在这方面多下一些工夫。

例如，有人询问过这样的问题：如果单纯使用 TPM 模式，可能还不如 U 盘模式的安全程度高。持有这种观点的人认为，如果使用 U 盘模式，至少密钥盘和计算机是可以分开保存的，这样，单独丢失了密钥盘或者计算机，都不会造成太大的损失（当然，硬件设备本身也值钱，但对于需要使用这个功能的人来说，设备中保存的数据可能更值钱）。但对于笔记本电脑用户，就存在一个很突出的问题：如果笔记本电脑本身带有 TPM 芯片，而我们又启用了 TPM 模式的 BitLocker，那么一旦笔记本电脑失窃，就等于窃贼同时获得了我们的硬盘及启动密钥。在这种情况下，BitLocker 功能可以提供的保护等于没有。

这种问题确实存在，但 BitLocker 功能的设计者早就考虑到了，此时可以使用混合模式的 BitLocker。这样除了 TPM 芯片外，还可以给系统再加一道锁，这道锁可以是一个独立于 Windows 账户的密码，或者是一个保存了启动密钥的 U 盘。这样，只要不是硬盘、TPM 芯片，以及 U 盘和密码同时全部失窃，系统的安全依然可以得到保障。

但依然有一个问题需要注意：恢复密码的妥善保管。无论是使用单纯的 U 盘模式、TPM 模式，还是任何一种混合模式，在启用 BitLocker 时设置的恢复密码一定要妥善保管，因为只要有恢复密码，无论什么模式的 BitLocker 加密，都将可以被绕过并重设。因此，恢复密码的安全性问题是绝对不能忽视的。

那么除了 U 盘模式外，其他几种模式的 BitLocker 分别是如何使用的？因为现在具有 TPM 芯片的计算机还不是很多，本书不准备详细介绍，只大概列出操作步骤，供感兴趣的朋友参考。

12.5.1 纯 TPM 模式

如果计算机主板上具有 1.2 以上版本的 TPM 芯片，就可以采用纯 TPM 模式的 BitLocker 加密保护系统。使用这种模式后，等于将硬盘、系统，以及计算机主板（或者扩展卡形式的 TPM 卡）捆绑在一起。只有特定 TPM 芯片存在的情况下才可以启动对应的操作系统。也就是说，如果台式机的硬盘被拆掉，安装到其他计算机上，将无法直接读取系统盘的任何数据。而且这种模式不需要用户在启动系统的时候提供任何密码或者 U 盘。如果在使用硬件 TPM 的模式对硬盘进行全盘加密后，还需要将硬盘退役，则只需要对 TPM 芯片进行初始化，等于将芯片中保存的密钥彻底清除掉，随后就可以放心地将硬盘处理掉，因为解密硬盘中数据的密钥已经彻底消失了。

要想使用纯 TPM 模式的 BitLocker，首先需要确保计算机上带有 1.2 版以上的 TPM 芯片。另外，在继续下面的操作之前，可能需要将计算机的主板 BIOS 更新到最新的版本，或者安装最新版本的 TPM 芯片驱动程序。详细信息请查阅主板或者 TPM 芯片的说明书。

如果确认计算机上的 TPM 芯片符合要求，请按照下列步骤对本机上的 TPM 芯片进行初始化：

STEP 01 运行“tpm.msc”，打开图 12-9 所示的 TPM 管理控制台。

STEP 02 单击图 12-9 中最右侧操作窗格中的“初始化 TPM”链接，随后可以打开图 12-10 所示的“初始化 TPM 安全硬件”对话框。单击“自动创建密码（推荐）”链接（因为 TPM 模式下并不需要手工输入这个密码，所以自动创建就可以满足要求）。

STEP 03 在随后显示的对话框中会显示 TPM 所有者的密码，单击其中的“保存密码”按钮，接下来会出现一个“另存为”对话框，需要为 TPM 所有者的密码指定一个保存路径和文件名。

STEP 04 当出现“完成”按钮后，表示 TPM 芯片的初始化工作已经结束，单击即可退出。

图 12-9　在这里对 TPM 芯片进行初始化

在初始化过程中，对创建的 TPM 所有者密码一定要妥善保管。在对 TPM 完成初始化工作后，就可以启用 BitLocker 了。需要注意的是，如果没有修改过有关 BitLocker 功能的组策略设置，则只能使用 TPM 模式的 BitLocker 加密。因此，在启用 BitLocker 的时候，系统并不会让我们选择使用哪种模式。

因为在启用 BitLocker 功能的过程中，大致的操作和上文介绍的 U 盘模式基本相同，因此，这里不准备重复说明。

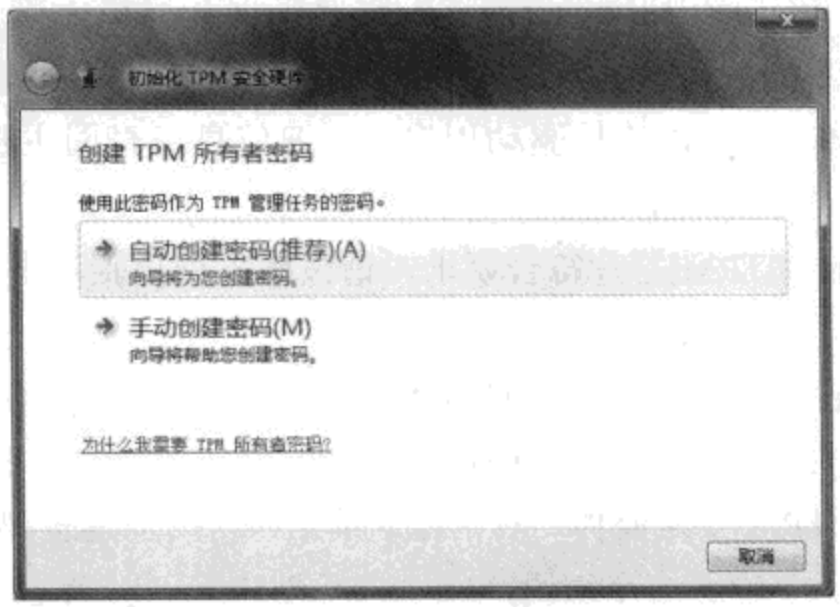


图 12-10　选择 TPM 所有者密码的创建方式

12.5.2　混合模式

上文已提到过，如果在笔记本电脑上启用了 TPM 模式的 BitLocker，那么笔记本电脑一旦失窃，BitLocker 功能对系统的保护将形同虚设。这时候可以考虑使用混合模式的 TPM，这样做可以获得更进一步的安全性，但易用性上会降低不少，因为同样要求我们每次启动系统的时候都能提供 U 盘或者 PIN 码。

毕竟安全性和易用性永远都是相对的，安全程度的升高不可避免地需要用易用性作为代价。因此，是否使用混合模式的 BitLocker，请根据数据的敏感程度和对安全的要求来决定。

混合 TPM 模式的 BitLocker 加密有以下两种模式。

- **TPM 芯片和启动 PIN 组合加密**　在纯 TPM 模式的基础上，再设置一个启动密码（PIN 码），这个启动密码由 4～20 位数字组成。每次启动计算机时，必须手动输入这个 PIN 码，然后和 TPM 芯片中的存储根密钥（SRK）结合起来，才能解密系统盘。
- **TPM 芯片和启动 USB 密钥组合加密**　在纯 TPM 模式的基础上，再设置一个启动密钥，这个密钥存放在 U 盘里。每次启动计算机时，必须提供保存密钥的 U 盘，然后和 TPM 芯片中的存储根密钥（SRK）结合起来，才能解密系统盘。

下文将分别介绍这两种模式。

1．TPM+PIN

默认情况下，在 Windows 7 中只能使用纯 TPM 模式的 BitLocker 加密。因此，首先需要对组策略设置进行一些调整，具体方法请参考上文。

至于 BitLocker 加密的启用方法，其实都是大同小异的，只不过在加密前的设置过程有些差别需要注意：

STEP 01　打开“控制面板”窗口，依次进入“系统和安全”→“BitLocker 驱动器加密”。

STEP 02 单击“启用 BitLocker”链接，随后可以看到图 12-6 所示的对话框。这些选项的作用如下：

- **使用没有附加密钥的 BitLocker**　纯 TPM 模式的加密。
- **每次启动时要求 PIN**　TPM 芯片和启动 PIN 码的混合模式加密。
- **每次启动时要求启动密钥**　TPM 芯片和启动 USB 密钥混合模式加密。

STEP 03 因为我们需要的是 TPM+PIN 的方式，因此，直接单击“每次启动时要求 PIN”按钮，随后可以看到图 12-11 所示的对话框。

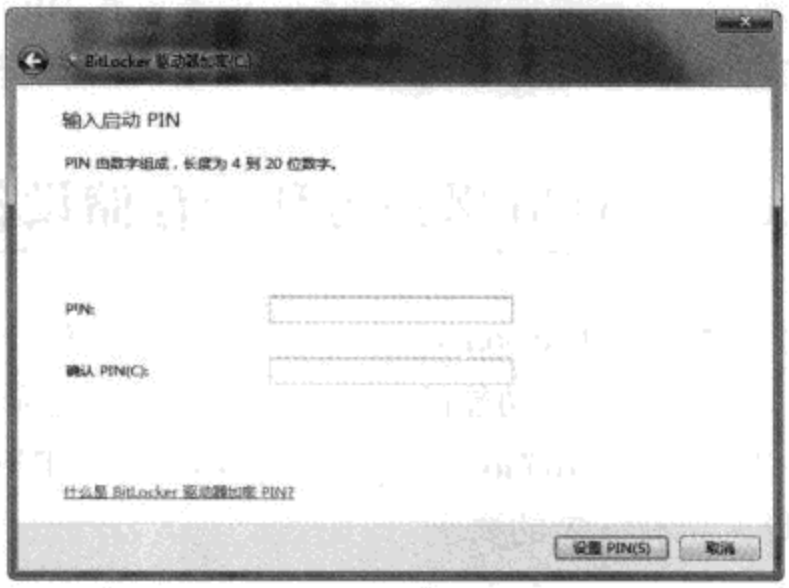


图 12-11　设置启动系统所需的 PIN 码

STEP 04 输入 PIN 码并确认，然后单击“设置 PIN”按钮即可。

接下来的步骤和 U 盘模式类似，设置恢复密码，进行加密。同样，加密过程需要很长时间。日后使用系统的时候，不仅要确保 TPM 芯片正常工作，而且必须在加载系统之前输入在这里指定的 PIN 码。

2. TPM+U 盘

对于 TPM+U 盘的模式，其操作上和 TPM+PIN 码的步骤基本类似，只不过需要在上一节中的第 2 步时单击“每次启动时要求启动 USB 密钥”按钮，然后将用于保存启动密钥的 U 盘连接到计算机即可。

在使用这种模式后，日后每次开机后不仅要确保 TPM 芯片的正常工作，而且必须预先将保存了启动密钥的 U 盘连接到计算机上。

在了解了上述两种混合模式后，可能有人会问，既然在使用混合模式的时候一样需要提供 U 盘，或者输入 PIN 码，那么 TPM 芯片到底还有没有存在的必要呢？当然有，在有 TPM 芯片参与的情况下，BitLocker 加密功能不仅可以有效地保护系统分区不被未经授权的访问或者脱机攻击，而且可以保证系统盘重要文件的“合法性”。

在有 TPM 芯片参与的 BitLocker 加密模式下，在加密系统盘的同时，加密程序会把主引导记录（MBR）、NTFS 卷的引导扇区、NTFS 引导代码、BitLocker 密钥等启动部件（这

些重要的启动部件并非全部保存在被加密的 Windows 安装分区中，还有一部分是被保存在未加密的“系统盘”中的）做一个“快照”保存在 TPM 芯片中。每次系统启动时，解密程序会自动将这些文件的内容与 TPM 芯片中保存的快照进行比较，只有发现这些启动部件没有发生变化的情况下，才会继续解密过程。

也就是说，有 TPM 芯片参与的 BitLocker 加密可以接管系统的引导过程，保证引导文件的完整性，并保证在操作系统完全启动好之前不被攻击。一旦发现这些重要的引导文件的内容和 TPM 芯片中保存的“快照”信息不相符（可能是硬件损坏或者被病毒感染导致，也有可能是用户自己的操作导致，例如安装多系统，或者更新 BIOS），就会提示用户，系统文件可能已经经过了篡改。而单纯的 U 盘模式 BitLocker 无法实现这项功能。

12.6 使用 BitLocker To Go 保护可移动存储设备

Windows 7 中包含了完整的 BitLocker 功能，不仅如此，还有一种针对可移动存储设备的 BitLocker To Go 功能。虽然这两个功能的名称类似，但属于完全不同的两种功能，而且对硬件的要求也不相同。BitLocker To Go 对硬件的要求较低；而 BitLocker 不仅要求特定的硬件设备，而且对硬盘分区也有一定的要求。

12.6.1 准备工作

虽然技术的发展使得通过网络共享文件成为一件非常简单快捷的事情，但由于各种原因，依然有很多人需要通过可移动存储设备在不同的计算机或不同的人之间共享文件。例如，USB 接口的移动硬盘、USB 闪盘等，这些设备通常是交换大量文件的首选方式，甚至有些人的日常工作也离不开此类设备，例如下班时间到了，发现自己还有重要的工作没有完成，直接带笔记本电脑回家比较麻烦，索性将工作所需的文件都复制到可移动存储设备中，回家继续工作。

这类可移动存储设备为了方便携带，其体积往往都非常小，尤其是 USB 闪盘，现在有些大容量 USB 闪盘甚至只有几毫米厚度。虽然便携性提高了，但丢失的可能性也随之增大。

用 EFS 加密吗？确实，EFS 加密是一种非常好的数据保护方法，而且只要是 NTFS 文件系统的硬盘分区，就可以直接使用（有关 EFS 的详细信息，请参考 5.4 节）。但是 EFS 却存在一个非常大的不足：密钥必须保存在本地计算机上。这就要求，如果将 USB 闪盘上的数据用 EFS 加密后，再插入其他计算机的 USB 接口，首先必须在初次加密的计算机上导出自己的证书（连同私钥），并将密钥导入到自己要使用的每台计算机上。如果忘了导入密钥，仅仅只是耽误工作，危险的是，将密钥导入临时使用的计算机而忘记将其删除，将造成密钥泄露。也就是说，EFS 并不是为了移动存储设备而设计的加密手段。

因此，最好有一种专门针对可移动存储设备的加密方式，而 BitLocker To Go 就是其中之一，可用于将可移动存储设备上的整个分区进行加密，并设置密码和恢复密钥文件。以

后每次读写该设备时，需要输入密码；如果忘记密码，则需要提供恢复密钥文件。

BitLocker To Go 的易用性要比 EFS 好很多，因为不再要求密钥必须保存在本地，只要记住密码，就可以自动派生出密钥，进而就可以在任何一台支持该功能的计算机上读写存储设备中的数据，而在这个过程中，数据都会维持加密状态。

如果希望用 BitLocker To Go 加密可移动存储设备，要求必须使用 Windows 7 操作系统，但加密后的设备不仅允许 Windows 7 对其进行读写，还可以通过组策略设置允许 Windows XP SP2/Vista/Server 2008 进行读取（在老版本系统上只能读取，无法写入）。因此，即使需要在其他计算机上使用该加密设备，也无须考虑操作系统问题。BitLocker To Go 加密功能向后兼容的操作系统非常广泛，基本上覆盖了 Windows 所有的主流版本。

BitLocker To Go 的使用没有什么特殊的要求，只要可移动存储设备的可用空间不小于 64 MB 即可。

12.6.2　对设备进行加密

如果希望使用 BitLocker To Go 加密 USB 存储设备，可按照如下步骤进行操作：

STEP 01 在“控制面板”中依次进入“系统和安全”→“BitLocker 驱动器加密”。

STEP 02 将希望加密的 USB 存储设备连接到计算机，稍等片刻，在图 12-12 所示的界面上，BitLocker To Go 选项下会列出可加密的设备。

STEP 03 如果设备上有多个分区，则所有的分区会分别列在“BitLocker To Go”的选项下。对于要加密的分区，单击其对应的“启用 BitLocker”链接。

STEP 04 系统会对所选设备进行一些检查，如果认为可以进行加密，则会显示图 12-13 所示的界面，在这里可以指定解锁该设备的方式。

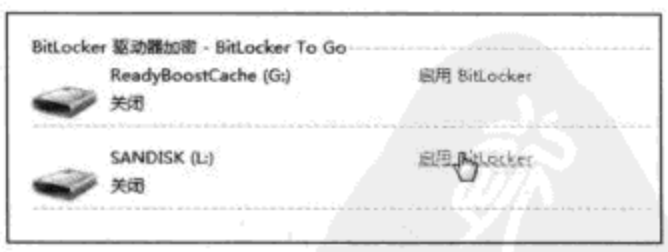


图 12-12　可被加密的设备都会直接列出来

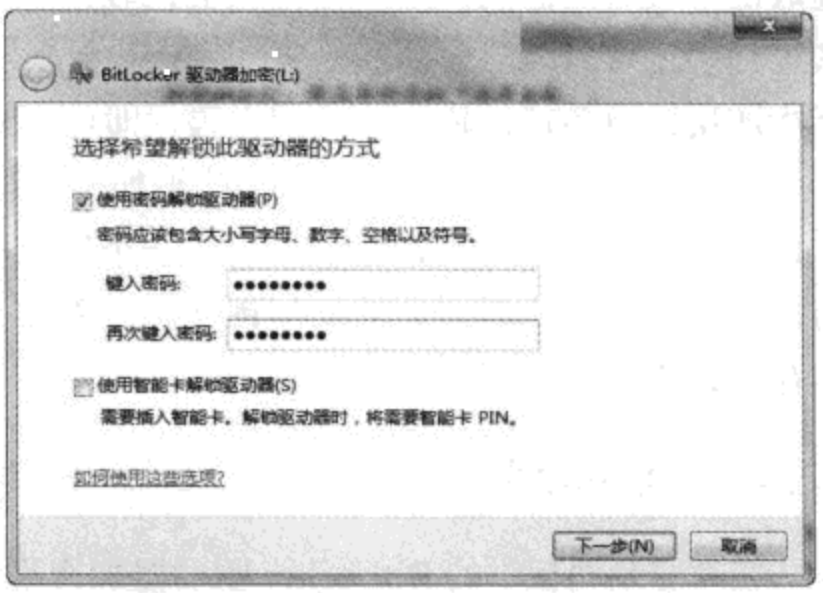


图 12-13　选择设备的解锁方式

STEP 05 这里有两种方式可以选择：密码或智能卡。其中，密码的使用更广泛，智能卡一般用于对安全性有较高要求的企业中，并且需要配套的系统才能实现。这里选中“使用密码解锁驱动器”复选框，并在下方的文本框中输入要使用的密码，然后单击“下一步”

按钮。注意，此处设置的密码就是以后每次访问该设备时需要提供的密码，因此，密码的安全级别一定要足够高。

STEP 06 随后需要在图 12-14 所示的界面上设置恢复密钥的处理方法。恢复密钥是一种备用的数据恢复方法，通常用于在忘记解锁密码后读取设备中的数据。此处提供了两种方式保存恢复密钥：将恢复密钥保存到文件，或直接打印出来。无论使用哪种方式，都要将恢复密钥妥善保管，因为任何人在获得恢复密钥后，都可以直接读取设备中的数据。

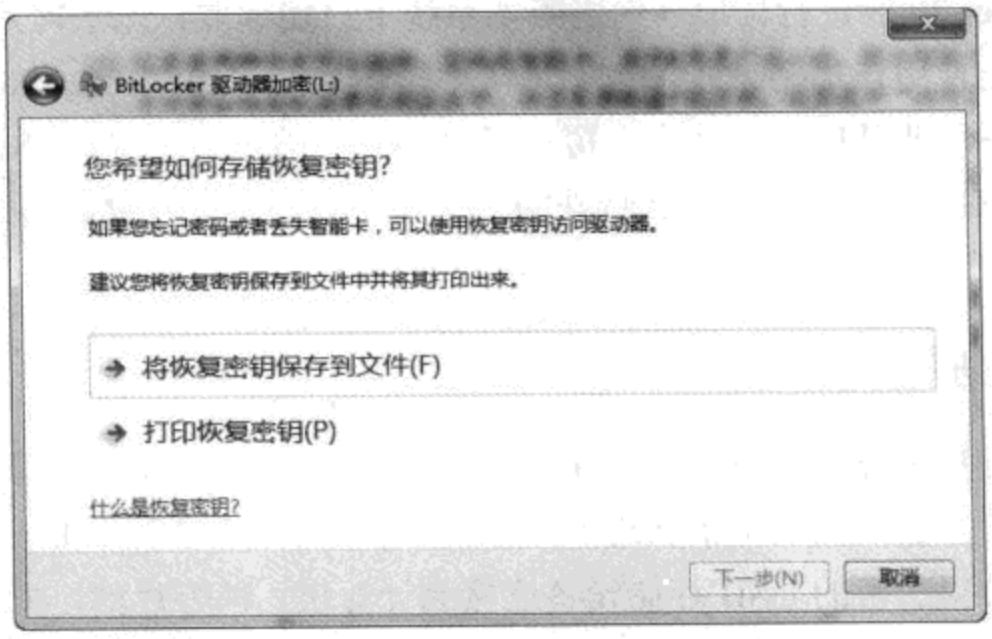


图 12-14　选择恢复密钥的处置方式

STEP 07 根据需求选择一种处理方式后，系统会要求选择密钥文件的保存位置，或选择要使用的打印机。处理完毕后，单击“下一步”按钮。

STEP 08 接着系统会询问是否开始加密该设备，单击“启动加密”按钮即可。这个过程取决于设备的总空间大小，通常会比较慢，加密过程中可以看到进度指示。另外，在加密过程中还可以随时暂停和恢复加密，甚至在暂停加密后，还可以将设备从计算机上断开，再次连接该设备后，输入正确的密码，即可继续加密过程。

当进度条显示完成后，该设备就被加密成功了。在本机上通过 BitLocker 驱动器和加密窗口可以看到被加密的设备上添加了一个锁的图标，但锁是被打开的，同时颜色也是黑白的，这表示该驱动器目前处于解锁状态。而在“计算机”窗口中，该设备表现的就和普通的存储设备一样，可以直接使用。

12.6.3　加密设备的管理

在“控制面板”的 BitLocker 驱动器加密设置页面上，对于加密后的设备，可以通过右侧的链接进行相关的设置。例如，如果希望在该设备上禁用 BitLocker To Go，就可以单击其右侧的“关闭 BitLocker”链接，在随后出现的 BitLocker 驱动器加密对话框中单击“解密驱动器”按钮即可。

如果单击“管理 BitLocker”链接，则可以看到图 12-15 所示的对话框，在这里可针

对该设备的加密选项进行配置（注意，只能影响该设备，无法影响其他加密设备）。

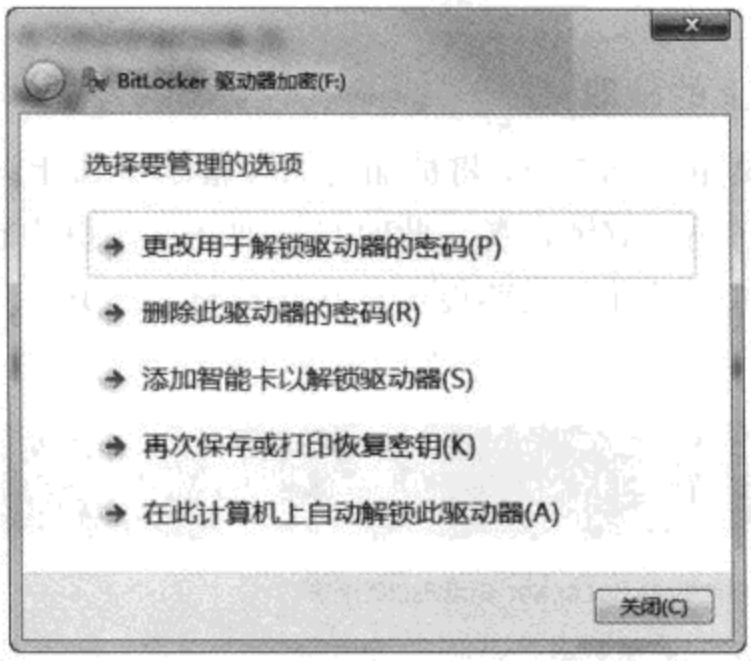


图 12-15　对特定设备的加密情况进行管理

各选项的用途如下：

- **更改用于解锁驱动器的密码**　通过该选项，可更改此设备的解锁密码，该密码可定期更换，以增强安全性。
- **删除此驱动器的密码**　如果该设备可通过两种方式进行解锁（密码和智能卡），则通过该选项可删除密码，但设备仍然处于加密状态，以后只能使用智能卡进行解锁。不过在没有设置智能卡时，无法删除密码。
- **添加智能卡以解锁驱动器**　如果在加密设备时只选择了密码解锁，但随后希望添加智能卡解锁功能，则可使用该选项。在单击该选项之前，需将智能卡插入读卡器，然后单击该选项，并按照屏幕上的提示进行操作。
- **再次保存或打印恢复密钥**　在加密设备时就已经设置过恢复密钥的处理方法，但如果当时准备的密钥丢失，则可以通过该选项重新获得恢复密钥。
- **在此计算机上自动解锁此驱动器**　通过使用该选项，以后在这台计算机上使用该设备时，就可以自动解锁，不需要每次都输入密码或提供智能卡。使用这一选项时需要谨慎，通常只建议在固定场所使用的计算机（例如家里或办公室的台式机）上使用该选项。另外，如果该设备已经被设置为在此台计算机上自动解锁，则该选项会变为“在此计算机上关闭对此驱动器的自动解锁”，选择该选项后，可删除本机保存的解锁密码，这样以后每次连接该设备后，就需要输入密码。

12.6.4　加密后设备的读取

默认设置下，被 BitLocker To Go 功能加密后的可移动存储设备可以在任何运行 Windows 7 系统的计算机上读取（前提是输入正确的解锁密码，或者提供智能卡）。但如果

希望设备在老版本 Windows 中能被读取（只读操作，无法写入），则需要在加密设备之前预先进行一些设置。

1. 在 Windows 7 上的读取

在任何一个版本的 Windows 7 中，将被加密的设备连接到计算机后，可以看到图 12-16 所示的界面，要求输入密码以解锁设备。此时只需要在文本框中输入加密时设置的密码，并单击“解锁”按钮即可。这样，只要设备不从计算机上断开，当前用户不注销，该设备就会一直保持解锁状态。

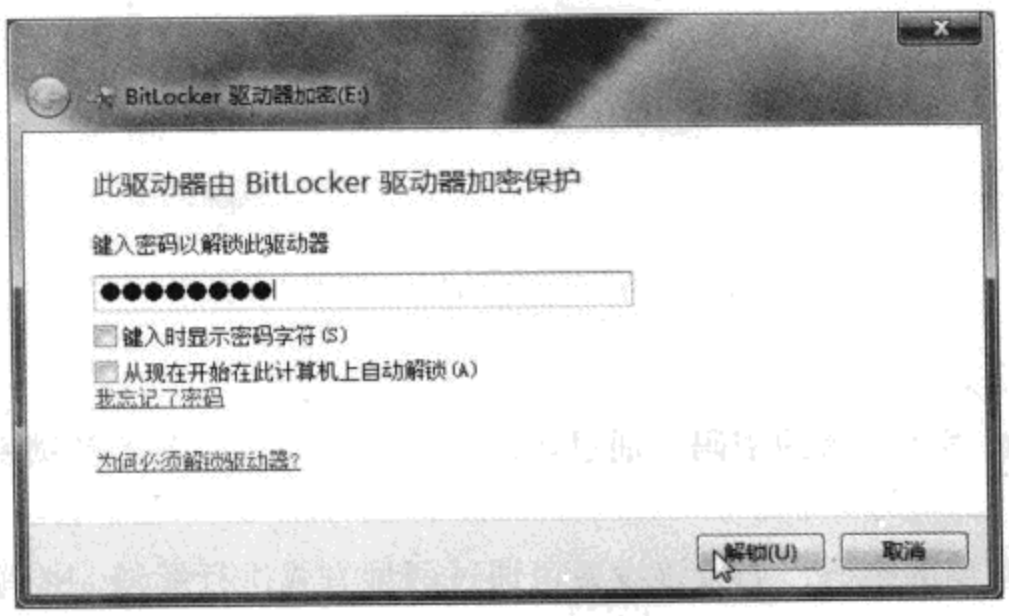


图 12-16　输入密码即可解锁设备

在该对话框中还有一个选项“从现在开始在此计算机上自动解锁”，如果选中该选项，以后在这台计算机上使用该设备时，将自动解锁，不需要输入密码。如果是他人或公用的计算机，不建议选择该选项。

在“计算机”窗口中可以看到，被锁定的设备的图标上有一个黄色的锁图标，并且锁是闭合的，同时窗口底部的细节窗格中显示的状态是“已锁定”。如果尝试强制打开该设备，将看到访问被拒绝的信息。

2. 在老版本 Windows 上的读取

如果是在老版本 Windows 中连接该设备，又会遇到怎样的情况呢？在 Windows XP/Vista 中具体的表现是一样的下面仅以 Windows XP SP3 中的情况为例进行介绍。

首先需要在 Windows 7 系统下对设备进行加密，具体操作如下：

STEP 01 根据需要，将设备格式化为 FAT/FAT32/exFAT 文件系统。

STEP 02 运行“gpedit.msc”，打开组策略编辑器，从左侧的树形图中定位到“计算机配置”→“管理模板”→“Windows 组件”→“BitLocker 驱动器加密”→“可移动数据驱动器”节点。

STEP 03 找到并双击打开“允许从 Windows 早期版本访问受 BitLocker 保护的可移动数据驱动器”策略。

STEP 04 选择“已启用”，并选中“禁止在 FAT 格式化可移动驱动器上安装 BitLocker To Go 读取器”选项。

加密好设备，并保存了重要文件后，如果需要在 Windows Vista/XP 等老系统中读取，则需要进行下列操作（在此以 Windows XP SP3 系统为例）：

STEP 01 下载并安装对应版本的 BitLocker To Go 读取器，地址为 http://tinyurl.com/ybkptur（这一步是必需的）。

STEP 02 将加密后的设备连接到计算机，随后将看到图 12-17 所示的密码输入框。

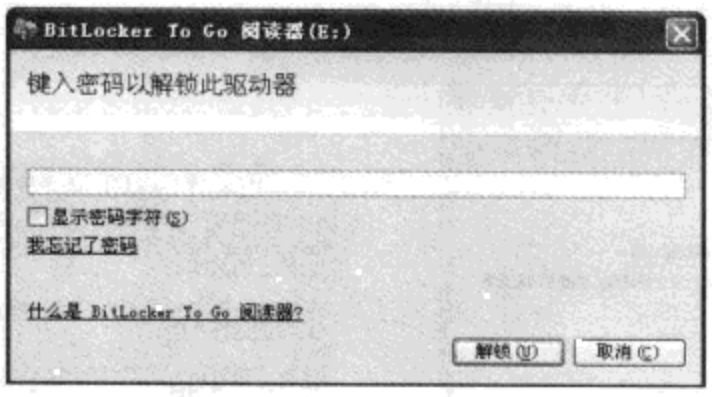


图 12-17　在这里输入解锁密码

STEP 03 如果 Windows 被禁用了自动播放功能，或者因为其他原因没有弹出自动播放菜单，可以直接在“开始”菜单的“所有程序”下单击“BitLocker To Go 阅读器”快捷方式，启动该工具，并输入密码和解锁。

STEP 04 如果密码正确，将看到图 12-18 所示的对话框，这里列出了设备上保存的所有内容，这些内容可以通过拖动复制到本地硬盘，但无法直接在设备上修改，也无法向设备中保存新的内容。

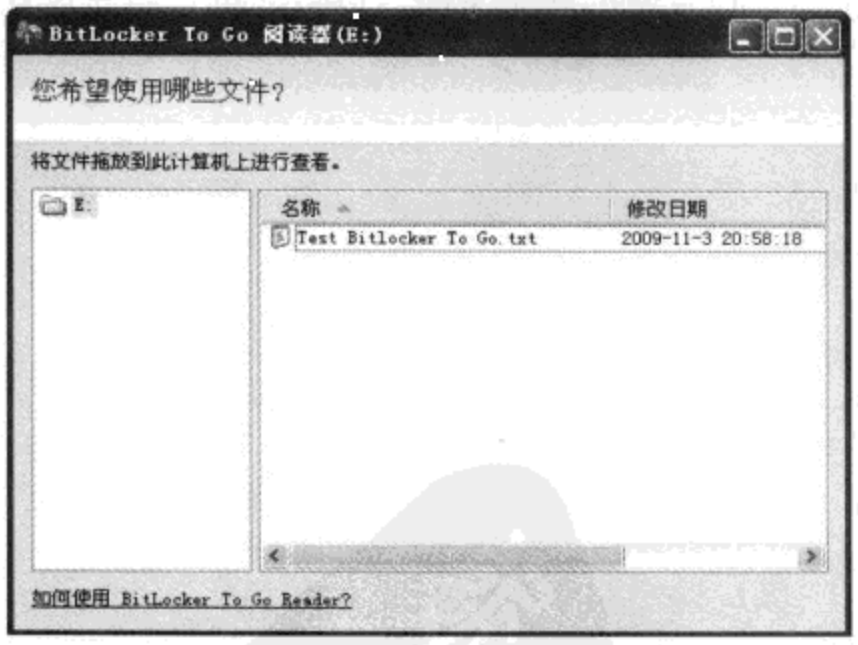


图 12-18　通过阅读器看到设备中保存的内容

12.6.5　忘记密码后的恢复

对于已经加密的设备，如果忘记了解密密码，则可以通过加密设备时获得的恢复密钥

进行恢复，具体过程如下：

STEP 01 将设备连接到电脑上，随后会出现用于输入解锁密码的对话框，在该对话框中直接单击“我忘记了密码”链接，随后将看到图 12-19 所示的恢复界面。

STEP 02 找出加密设备时保存的恢复密钥（可能是硬盘上的一个纯文本文件，或者是打印的一张纸），留意“可以通过以下方式识别您的恢复密钥”字样后面显示的设备标记。

STEP 03 在恢复密钥文件或纸张中，应该可以看到图 12-20 所示的内容，请留意恢复密钥中显示的标记与图 12-19 显示的标记是否一致。如果一致，证明该恢复密钥是这个设备的；如果不一致，则证明这个密钥并不是这个设备的。

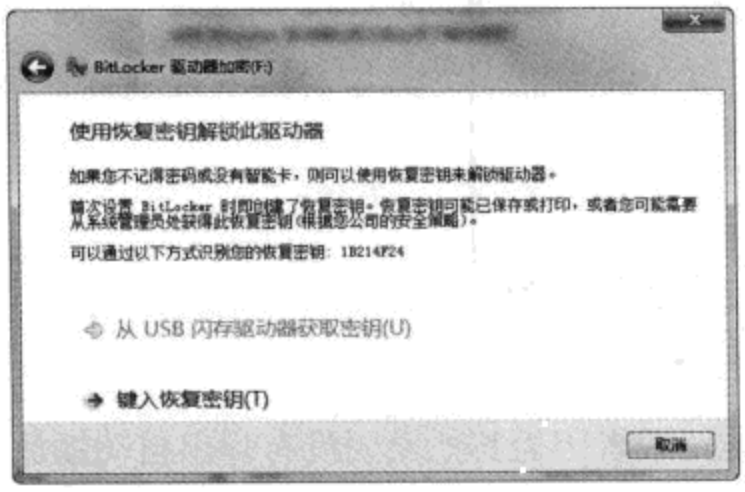


图 12-19　选择恢复选项

图 12-20　根据标记查找正确的恢复密钥

STEP 04 在图 12-19 中单击“键入恢复密钥”按钮后会看到密钥输入框，请在文本框中输入恢复密钥文件中显示的“BitLocker 恢复密钥”，然后单击“下一步”按钮。

STEP 05 随后应该能看到“管理 BitLocker”按钮，请单击该按钮，并单击“更改用于解锁驱动器的密码”按钮，设置新的解锁密码，以后即可使用新设置的密码解锁该设备。

CHAPTER

13

第 13 章　备份和还原

虽然 Windows 自带的很多功能及大量第三方软件都可以保护我们的系统和数据的安全，然而这些措施有时候并不是万能的。例如，最常见的问题是硬件损坏，我们可能很在意自己的数据安全，因此，采取了各种措施保护计算机系统和文件不被破坏，并且平时使用都是小心翼翼的。然而某天开机时突然发现系统无法启动了，找人检查后才知道硬盘损坏，其中所有的数据都丢失了。

与其亡羊补牢，不如提前就做好准备，以便应对任何可能发生的突发事件。

有关备份和还原的知识，本书主要讨论两方面的内容：文件的备份和还原，以及系统的备份和还原。通过备份文件，就可以在出现一些不希望的事件（例如错误地删除了重要文件，或者感染病毒导致文件损坏）后从备份中将重要文件恢复出来。而对于系统的备份，主要目的是为了在系统正常运行的时候将所有的系统文件都备份起来，并在系统出现问题后通过备份将系统还原到之前的正常状态，这样可以避免重新安装系统和应用程序、安装补丁和修改设置的麻烦。

13.1　文件的备份和还原

相对系统的备份和还原，文件的备份和还原更重要。毕竟，系统如果不备份，损坏后还可使用系统安装盘重新安装，然后重新安装其他软件，这样虽然麻烦，但依然可以解决问题。而文件的备份和还原就不同了，一旦文件或者文件备份丢失，很多内容可能根本找不回来，例如，公司过去若干年积累的各种资料、家中小孩从小到大的照片和视频等。因此，我们可以不重视系统的备份，但绝对不能轻视文件的备份。

在文件备份方面，很多人都抱有侥幸的心理，认为备份操作太麻烦，而文件损坏或丢失的几率很小。对于抱有这种观点的人，一次文件丢失就会彻底扭转这种错误的看法。也许丢失的几率只有 1%，可一旦遇到这 1%的可能性，造成的损失就是 100%。如果计算机中保存了自己比较重要的文件，最好还是经常备份。

虽然数字化保存的文件更易于使用，不过在管理和维护上并不容易。相信阅读本书的很多朋友的家中都可以找到十几年甚至几十年前的纸质图书文档或者泛黄的老照片，可是

在计算机硬盘上能找到多少几年前创建的文件呢？

13.1.1 文件备份的重要原则

文件的备份操作很简单，只要使用 Windows 自带的备份程序就可以完成，但要做好备份，并不是一件简单的事情。

13.1.1.1 备份什么内容

在决定备份重要文件之前，首先需要明白一个问题：备份什么。到底什么才是自己最重要的文件？对于不同的人，答案各不相同。有人可能希望备份公司计算机中的工作文件和电子邮件，有人可能希望备份自己的家庭成员照片或者视频文件。因此，在决定备份之前，请首先将要备份的内容都记录下来。

在讨论这个问题的时候，首先要提一提很多人在使用计算机时一个很不好的做法，一些人可能是为了沿袭以往的使用习惯，喜欢在硬盘上创建很多分区，并且在创建的时候还有很好的规划，这个分区保存照片，那个分区保存视频，另外一个分区保存文档或者网络上下载的文件。结果在实际使用的过程中，就完全没有章法了，今天把文件保存在这里，明天把文件保存在那里。虽然随意保存文件在使用的时候很方便，可是在后期的管理、查找及备份时会带来很多麻烦，我们可能要翻遍硬盘上的每个文件夹，看看自己的重要文件都被保存在哪里，而且这样做很容易造成疏漏。我们可能觉得自己已经把各种重要的文件都备份好了，可硬盘出故障后，打算从备份中还原文件的时候才发现，怎么最重要的文件竟然没有被包含在备份中。

所以，在开始备份之前，还是先养成良好的使用习惯。

在 Windows 7 中，新增了一个叫做库的功能，库实际上属于文件夹的虚拟视图。我们可以将不同的文件夹添加到一个库中，这样看起来，就可以通过一个库访问所包含的所有文件夹，但实际上文件还位于不同的文件夹或不同硬盘的分区，甚至不同的计算机中。而 Windows 7 自带的备份功能完全可以针对库进行。因此，就算真的需要将不同的文件保存在不同的位置，也至少请将它们添加到一个或多个库中，这样备份和恢复起来会更容易一些。

Windows 7 中的“库”在功能上类似于以往很多人所熟知的“文档”等默认文件夹，然而很多人并没有注意到这个文件夹的作用，相反，很多人还有一种很有趣的想法：硬盘是我自己的，文件也是我自己的，我愿意保存在哪里就保存在哪里，为什么要让别人来给我安排？当然，每个人可以把自己的重要文件保存在自己愿意使用的任何地方，但为了方便日后的备份和使用，就算不使用系统提供的默认位置，建议至少还是集中保存比较好。

另外有一个问题需要注意，对于这个专用的文件夹，默认的位置位于每个账户的配置文件夹中，也就是说，位于安装了 Windows 的硬盘分区上。这样做的主要目的是为了让每个账户自己的“文档”文件夹是相对独立的，每个人看到的自己的“文档”文件夹中都只

有自己的文件，不会有别人的文件。然而这样做会造成一个问题：如果 Windows 崩溃了，需要重新安装系统，或者使用备份还原系统该怎么办？按照默认的设置，在重装或者还原之前，还必须通过各种方法将系统盘保存的重要文件都复制到其他硬盘分区或者计算机上，那么一般会使用哪些办法？把硬盘拆下来，连接到其他计算机上复制？还是使用 Windows 安装光盘引导系统，进入故障恢复控制台，然后使用命令行界面来复制？无论哪种方法，都比较麻烦，而且很容易出错。

因此，建议将“文档”等默认文件夹重定向到其他位置，例如重定向到非系统盘。经过这样的操作，“开始”菜单或者其他地方还有“文档”这个快捷方式，但单击这个快捷方式后，打开的是位于非系统盘的“文档”文件夹。这样，就算系统有问题需要重装或者还原，我们也不用操心文件的转移工作，因为文件本身就没有保存在系统盘上，因此，我们只需要直接重装或者还原系统，然后将新系统中的“文档”文件夹重定向到非系统盘的“文档”位置即可。

为了更改 Windows 7 中“库”和“文档”等默认文件夹的保存位置，硬盘还需要满足一个条件：除了一个安装 Windows 的分区外，至少还有一个分区可以用来保存文件具体应该如何操作？

在 Windows 7 中，如果想要将“库”重定向到其他位置，可以这样操作：

STEP 01 打开“计算机”窗口，窗口左侧的导航栏中将列出系统自带的以及我们自己创建的库（如图 13-1 所示），单击每个库对应的节点，即可看到该库中包含的所有内容。

图 13-1　系统中已经创建的库

STEP 02 每个库可能会包含多个不同的位置，这些位置可能来自同一或不同硬盘分区上的文件夹，甚至可能包含局域网上其他计算机上的共享文件夹。而这里的目的就是将库中包含的位于系统盘上的文件夹找出来，并重定向到其他位置。因此，对于每个库，请首先单击进入该库，然后单击左上角的“×个位置”链接，随后即可看到该库包含的所有文

件夹的位置（如图 13-2 所示）。

图 13-2　查看每个库包含的文件夹位置

STEP 03 如果库中包含了系统盘下的文件夹，并且这些文件夹中保存了重要文件（例如图 13-2 中的“C:\User\liuhui\Videos”文件夹），请首先在非系统盘上方便的位置创建一个文件夹，然后将这些文件夹中的文件都复制到非系统盘中，接着单击“添加”按钮，将非系统盘中的文件夹加入到库中。

STEP 04 随后，选中每个系统盘下的文件夹，并单击“删除”按钮，将其从库中删除。

STEP 05 在添加好的某一非系统盘文件夹中单击鼠标右键，从右键菜单中选择“设置为默认保存位置”，并单击“确定”按钮。

经过上述操作，库中的所有内容都可以保持原有的结构，但所有位于系统盘下的文件和文件夹都已经被转移到非系统盘中。不过，实际使用时不会有任何变化。

窍门　什么是“默认保存位置”

前面已经介绍过，库实际上属于文件夹的一种虚拟视图，库中可以包含位于不同位置的文件夹。举例来说，如果向某个库中添加了“c:\folder1”、“d:\folder2”、“e:\folder3”，以及“\\FileServer\ShareFolder”这 4 个位置，那么在打开该库后，就可以直接看到 4 个文件夹分别对应这 4 个位置。可想而知，对于这 4 个文件夹，文件的读写操作实际上都会直接应用于上述 4 个位置。不过，如果将新的内容直接保存到该库的根节点下，这样的文件会被保存到哪个位置？这是由“默认保存位置”所决定的。如果将“d:\folder2”设置为默认保存位置，那么库根文件夹下保存的文件就会出现在“c:\folder2”文件夹中。因此，为了便于使用，最好将每个库的默认保存位置都设置为非系统盘位置。

虽然 Windows 7 中新增的库功能为我们的使用提供了很大便利，但传统的“文档”等默认位置依然被保留。这可能是为了照顾老程序而考虑的，因为很多程序的默认打开和保

存位置都是“文档”文件夹。毫无疑问，默认情况下，“文档”文件夹以及其他类似的默认位置的位置也在系统盘下，因此，我们还需要将它们重定向到非系统盘。具体做法如下：

STEP 01 打开“开始”菜单，并单击右上角照片下方的用户名，随后 Windows 资源管理器会自动打开当前用户的配置文件（如图 13-3 所示）。

图 13-3　Windows 7 中的默认保存位置

STEP 02 这里列出的每个文件夹都是可以重定向的，而且可以分别重定向到不同的位置。这些文件夹的作用请参考表 13-1。

表 13-1　文件夹名称及其作用

文件夹名称	作　用
保存的游戏	用于保存支持该功能的游戏的存盘记录
联系人	用于保存联系人信息，这些信息可以被 Windows Live Mail 或者其他支持的程序所使用
链接	用于保存 Windows 资源管理器左侧的“收藏夹”内容
视频	用于保存视频文件
收藏夹	用于保存 Internet Explorer 的收藏夹内容
搜索	用于保存搜索功能创建的虚拟文件夹内容
图片	用于保存图片文件
文档	用于保存文档，类似老版本 Windows 中的“我的文档”
下载	Internet Explorer 下载文件的默认保存位置
音乐	用于保存音频文件
桌面	用于保存桌面上创建的文件、快捷方式等内容

STEP 03 对于想要重定向的文件夹，只要用鼠标右键单击它，选择“属性”，打开“属性”对话框，随后打开“位置”选项卡，单击“移动”按钮，即可为其指定新的位置。

经过上述的设置后，即可将所有重要的文件夹都重定向到非系统盘，实现更简单的使用和备份/还原。

13.1.1.2 备份到哪里

如果使用 Windows 自带的备份程序，可以将文件备份到本地硬盘、网络共享、软盘、U 盘、移动硬盘上，对于 Windows 7，还可以直接将文件刻录到光盘中。

很多人可能习惯于直接将备份文件保存在本地硬盘上，觉得这样不需要使用额外的设备，比较方便。可一旦硬盘出现故障，就算有备份文件也无法使用。因此，如果重视文件的安全性，就一定要注意，备份文件最好能做到异地保存。

另外，在选择备份文件的保存位置时还需要考虑备份介质的可靠性。例如，很多人习惯将一些家庭照片直接刻录到光盘上保存，虽然刻录光盘的制造商通常都会宣称刻录盘上的数据可以保存超过 50 年，但实践证明，对于一些质量不佳或者保存环境不好的刻录光盘，一两年之后，其中的数据就无法读取了，甚至有些光盘还会发霉。

那么有人可能会问了，备份到专用的硬盘上好不好？虽然硬盘的可靠性要比光盘高，但也不是绝对安全的。例如，硬盘一般只有不超过 5 年的质保，而且一个批次的硬盘中可能有一两块次品，如果我们遇到了，并且硬盘在保存了备份数据后坏掉了，这也是没有办法的事情。

因此，最理想的办法应该是将重要的文件同时备份在多种不同的介质上。例如，专门准备几张可复写的刻录光盘和专用的移动硬盘来保存备份文件，并将备份介质分别保存在不同的地方。这样，就算其中一种介质坏掉无法使用，至少还可以从其他介质上还原数据。

- 如果要将文件备份到光盘上，为了节约成本，建议使用高质量的可复写光盘。同时取决于数据的重要程度，可以将同样的备份保存在多张光盘上，这样就算一张光盘坏了，还可以使用其他光盘。另外，为了保证高可靠性，同一张刻录盘使用一段时间（半年或者一年，主要取决于备份数据的写入频率和刻录盘本身的质量，以及保存环境等因素）后建议更换，因为可复写刻录光盘的擦写次数也是有限制的。
- 如果要将文件备份到移动硬盘上，建议使用专门的一个移动硬盘来保存备份数据，平时最好不要使用这个移动硬盘作为他用。因为使用时可能发生各种意外，导致硬盘损坏（例如病毒感染或者硬盘跌落撞击损坏），只在需要备份和还原的时候才使用这块移动硬盘。
- 网上有很多提供在线存储服务的网站（也就是最近很热门的“云存储”概念），将文件存储在这些地方更加可靠，因为提供这些网络服务的公司通常都会实施非常妥善的文件备份机制，并且自己的文件可能会同时存储在全球多个不同的位置，其可靠性更高，所以，这种方式也非常适合普通用户的文件备份。然而，毕竟自己的重要

数据被他人掌控着，如果服务商停止服务，或者因为各种原因导致上传的文件被他人访问到，依然会造成不少的麻烦。因此，在使用此类服务时一定要慎重。

最后，还应该考虑备份介质的读取问题。建议随着技术的发展，及时更换自己的存储介质。例如，现阶段我们可能会使用 DVD 光盘备份文件，当蓝光（民用领域的一种最新技术的光存储介质，容量更大，速度更快，但目前的价格也较高）设备普及后，请尽快将 DVD 光盘上的备份文件迁移到新的介质上，以免日后遇到无法读取备份介质的尴尬。

13.1.1.3　怎么备份

一般说来，在进行备份之前应该创建一个切实可行的备份计划。例如，多长时间进行一次备份，具体的备份方式是什么。另外，为了保证随时可以将文件都还原出来，需要采用什么措施保证备份文件的状态总是最新的。

- 一般来说，对于那些需要频繁更改的文件（例如，本月工作过程中需要用到的文件），建议每周进行一次完整备份，然后每天在下班后进行一次增量备份。
- 对于不需要频繁更改的文件（例如，去年工作中用到的文件，虽然现在已经暂时不需要访问了，但还是需要将相关的文件都归档保存好），则可以进行一次完整备份，并将备份文件复制到多种不同类型的介质上，分开保存。
- 还有一种比较特殊的文件，主要是家庭用户使用的，那就是不需要再次被修改，但是需要经常访问的文件，例如家庭数码照片或者家庭录像。对于这种文件，不仅要保证文件的安全，而且要保证便捷的可访问性。因此，可以定期将其全部的文件手工复制到脱机存储的介质（例如，移动硬盘或者刻录光盘）上，但同时在本地硬盘上保留副本。这样，平时浏览的时候可以使用本地硬盘上的副本，如果本地硬盘出现故障或者文件被错误地删除，还可以从备份中进行恢复。

13.1.2　文件的备份和还原

在上文中已经针对不同需要的文件列出了不同的情况，在这些情况下分别需要怎样的备份和还原策略，在本节会分别进行说明。

13.1.2.1　备份和还原需要频繁变动的文件

对于需要备份和还原频繁更改的文件的环境，可以假设一个这样的环境：因为工作的关系，公司的计算机里保存了很多重要的文件，这些文件都位于“文档”文件夹中，并且变动很频繁，例如，老文件可能被修改或删除，同时可能会加入更多新的文件。这些文件对工作的正常进行都是至关重要的。

如果需要进行这样的备份，建议在每个工作日对文件进行一次备份。备份的文件可以保存在一个专用的移动硬盘中。具体的做法如下：

STEP 01　打开“开始”菜单，依次打开“所有程序”→“维护”→“备份和还原”，随后可以看到图 13-4 所示的备份和还原主界面。

STEP 02 单击“设置备份”按钮，随后会启动备份程序，程序首先会对系统进行分析，稍等片刻后，可以看到图 13-5 所示的界面，在这里需要选择用于保存备份文件的设备或位置。

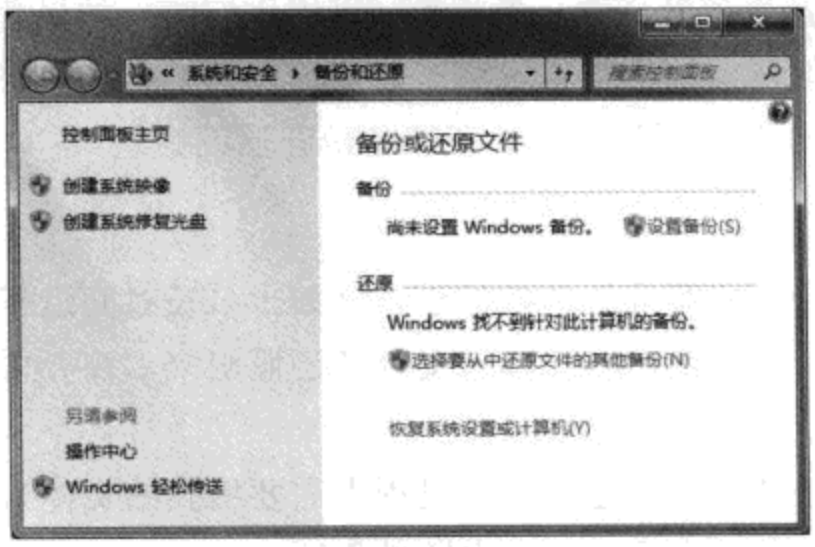


图 13-4　备份和还原主界面

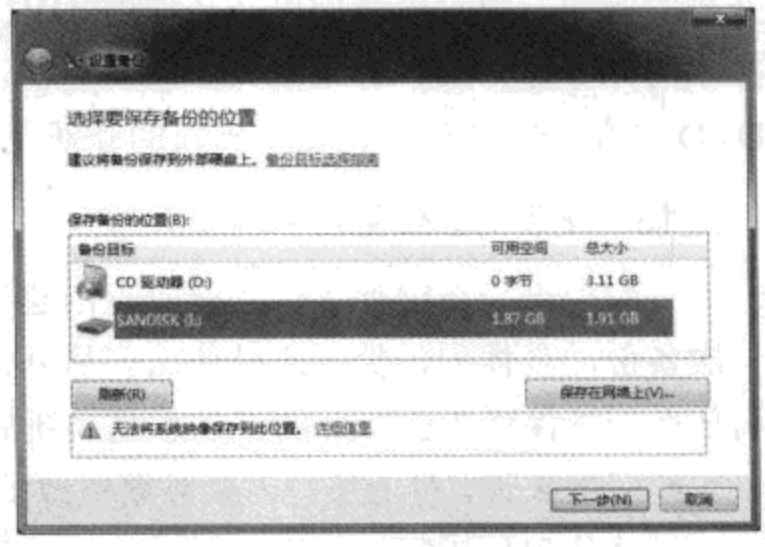


图 13-5　选择备份文件的保存位置

- 如果希望将备份保存到可移动存储设备（例如移动硬盘或 U 盘）上，请将其连接到计算机，并单击“刷新”按钮，令其显示到列表中，然后在列表中单击选中它。
- 如果希望将备份保存到本地硬盘分区中，也只需要在设备列表中将其选中即可。在这里只能选择要使用的设备，备份程序会自动在设备的根目录下创建一个文件夹来保存备份文件，不能指定将备份文件保存在设备的哪个文件夹下。
- 如果希望将备份保存到刻录光盘上，请在刻录机中放入空白光盘，然后从设备列表中将其选中。如果使用光盘保存备份，备份文件的容量如果比较大，一张光盘容纳不下，备份程序还可以自动将文件拆分刻录到多张光盘上，我们只需要按照屏幕上的提示提供新的刻录盘即可。
- 如果希望将备份保存到网络共享文件夹中，请单击“保存在网络上”按钮，并在随后出现的对话框中选择网络位置，输入用于写入该位置的用户名和密码，并单击“确定”按钮。

选择好之后，单击“下一步”按钮。

STEP 03 接下来需要选择要备份的内容，Windows 7 的备份工具提供了两个选项：“让 Windows 选择”和“让我选择”。对于前者，将无法自己选择要备份的内容，备份工具会自动对所有的库、桌面，以及系统数据进行备份，通常，这样的备份将包含大量的内容，并占用大量的备份空间，因此，通常不建议使用。以本例来说，我们只需要备份“文档”等特定的几个文件夹，因此，请选择“让我选择”，然后单击“下一步”按钮。

STEP 04 随后可以看到图 13-6 所示的界面，在这里可以选择要备份的内容。

为了便于选择，备份工具已经将所有的数据内容（实际上也就是“库”）列出在“数据文件”类别下，此时，如果系统中有多个用户，每个用户的库都会列在这里。我们可以根

据实际需要选择是否备份别人的库，以及具体要备份哪些库。如果以库为单位选择要备份的内容，则所有包含到库中的内容无论位于本地硬盘的哪个位置，或者位于网络上，都会被备份。

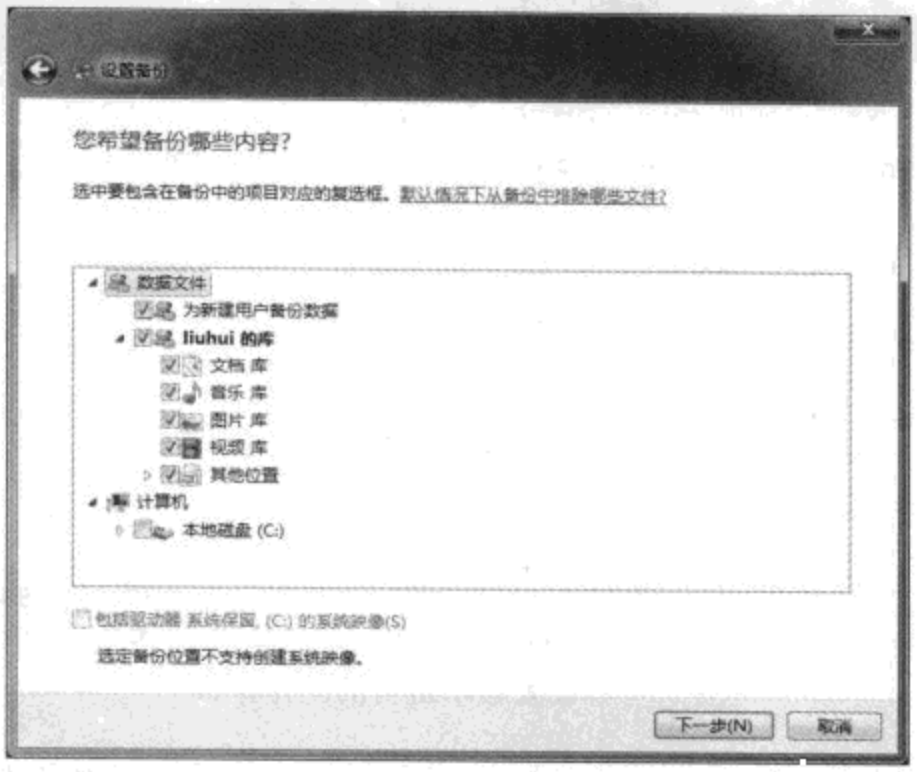


图 13-6　选择要备份的内容

窍门　什么是“为新建用户备份数据”？

备份工作通常只需要设置一次，并设定好计划，以后系统就会按照计划自动进行备份。如果在设置好备份后新建了用户账户，这些账户的文件如何进行备份？难道每次添加新账户后都重新调整备份设置？其实并不需要这么麻烦，只要选中“为新建用户备份数据”选项，这样以后每次新建账户，备份工具都会自动将该用户的所有库都包含到备份中。

如果希望备份其他内容，例如，没有被添加到库中的文件夹，则可以在“计算机”选项下选择，这里会列出所有的本地硬盘分区，并且每个分区前会显示一个箭头，单击后即可展开。这样就可以按照需要添加其他文件夹到备份中。

取决于所选的保存位置，某些情况下，“包括驱动器×××的系统映象”选项将变为可用。如果选中该选项，那么在备份文件的同时，备份工具还将备份整个系统。通常不建议使用该选项，因为在大部分情况下，系统只需要备份一次，并不需要频繁备份。因此，我们只需要在安装好系统和程序，并做好所有的设置后，单独对系统进行一个备份即可。平时只需要确保文件得到妥善备份，就可以在遇到意外后尽快恢复。如果在备份文件的时候也选择“包括驱动器×××的系统映象”选项，则每次备份的时候，都会对系统中有变化的文件进行备份，这样做无疑会延长备份所需的时间，并占据大量的备份空间。

STEP 05 选择好后，单击“下一步”按钮，并单击“更改计划”链接，随后可以看到图 13-7 所示的界面，在这里可以设置自动备份的工作频率和其他安排选项。

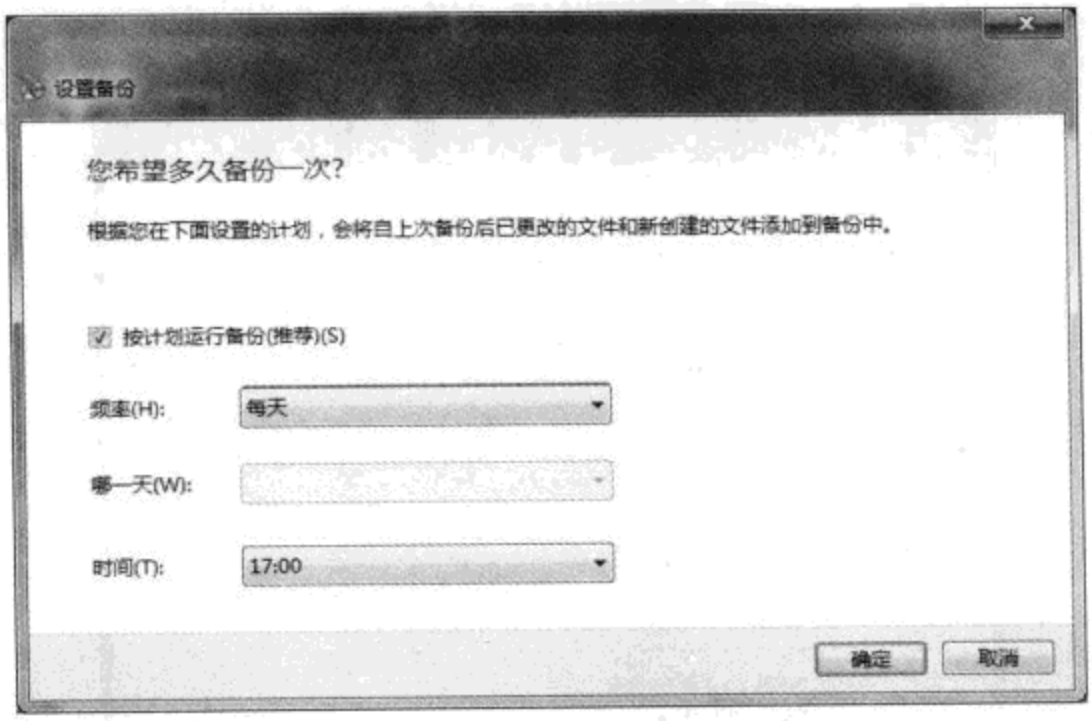


图 13-7　设置自动备份的工作参数

建议通过文件的变动频率来决定备份的执行频率。如果每天都有很多文件变动，建议从“频率”下拉菜单中选择“每天”，然后从“时间”下拉菜单选择备份开始的时间，例如，可以选择下班前一小时。设置完毕后单击“确定”按钮。

STEP 06 单击“保存设置并运行备份”，系统将会自动开始备份符合条件的文件。如果是第一次备份，那么备份工具会自动创建完整备份，日后的备份则会用类似“增量”的方式完成，也就是说，只备份自从上次成功备份后变动过的，或者新创建的文件，这样可以减少备份文件的体积，以加快备份的速度。

在完成上述操作后，就不用关心日后的文件备份工作了，Windows 的备份程序会在我们设定好的时间里自动运行，并自动备份文件。但依然需要注意，如果在上面的操作中选择将备份文件保存在可移动存储设备或者光盘上，那么还必须在备份开始之前将可移动存储设备连接到计算机，或者将刻录盘放入刻录机中，如果备份文件的体积比较大，可能还需要预先准备多张刻录盘。

如果在预计的时间内因为无法访问备份介质而导致备份失败，Windows 7 的操作中心内会显示相关的信息。在看到这样的信息后，只需要将备份介质连接到计算机，再次打开备份和还原主界面，单击“重试”按钮即可。

设置好备份，并完成初始备份后，备份和还原主界面上将显示有关该备份的相关信息（如图 13-8 所示）。例如，上次备份和下次计划备份的时间、备份介质的空间使用情况，以及具体的备份设置等信息。如果因为某种原因需要更改备份任务的设置，可以再次打开备份和还原主界面，并单击“更改设置”链接，随后即可按照上文介绍的设置备份的相关步骤，重新修改与备份有关的所有设置。

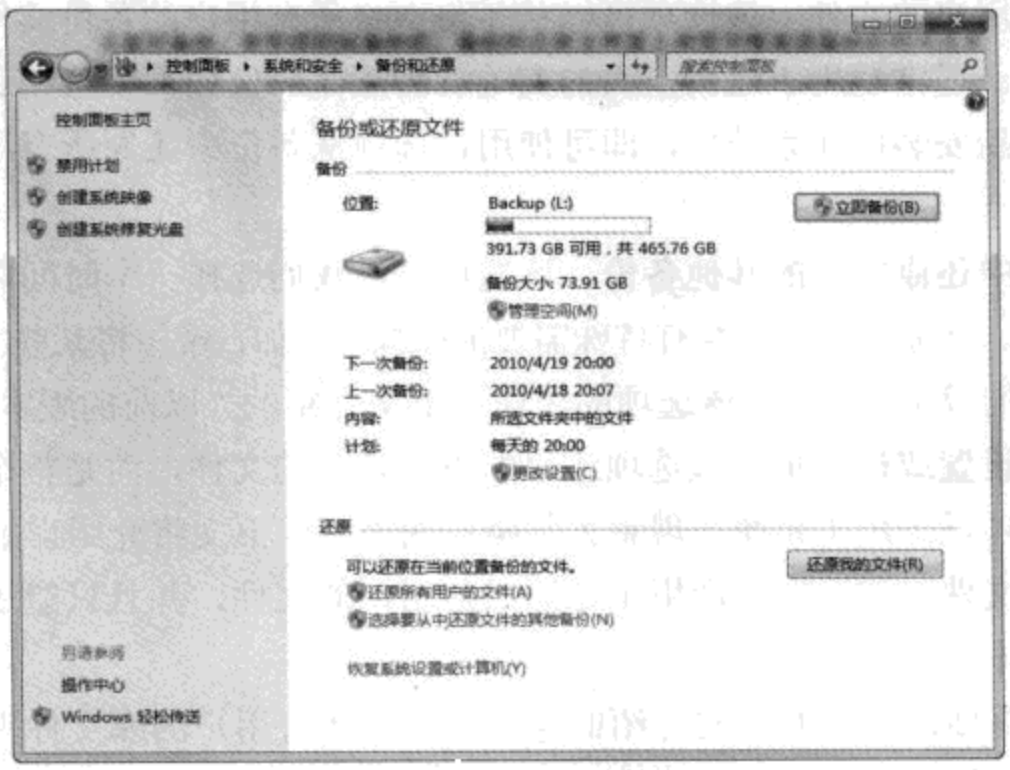


图 13-8　查看备份的设置情况

同一个备份介质在经过长时间的使用后，可用空间会逐渐降低，并将无法用于继续保存备份内容。此时可以根据需要将老的备份内容手工删除，为新备份腾出足够的空间。为此，请在图 13-8 所示界面上单击“管理空间”链接，随后可以看到管理 Windows 备份磁盘空间对话框，这里会列出备份文件的保存位置，以及不同类型文件的空间占用情况。如果需要删除以前的备份，可以单击“查看备份”按钮，随后可以看到图 13-9 所示的界面，在这里，备份工具会将所有的备份按照一定的时间跨度进行分组排列。例如，如果设备中包含了数个月的备份，则会按照月份进行分组；如果包含了数周的备份，则会按照星期进行备份。在这里，我们只需要选中最早的时间跨度，然后单击“删除”按钮即可。

经过上述操作，文件即可得到妥善的保护。虽然每个人都希望自己永远不需要还原数据，但意外总是会发生，如果需要从备份中还原文件，请按照下列步骤操作：

STEP 01　打开“备份和还原中心”，在“还原”选项下可以看到与还原操作有关的不同设置（如图 13-10 所示）。这些选项的作用和含义分别是：

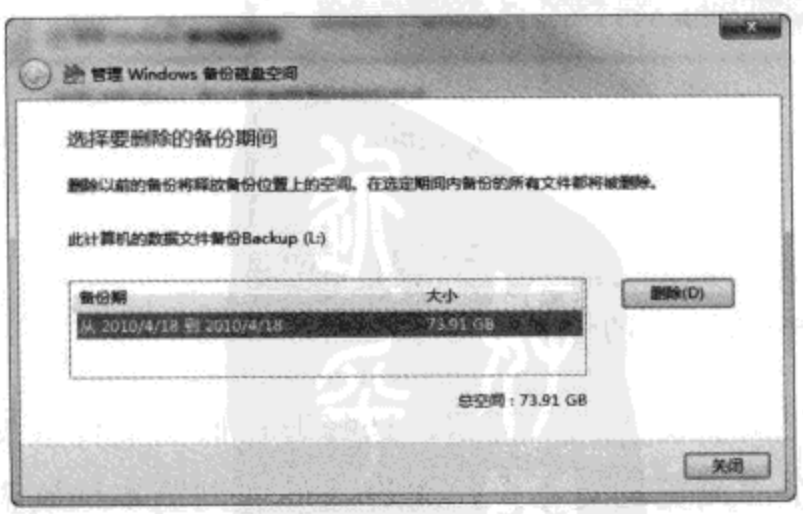


图 13-9　删除老备份即可释放空间

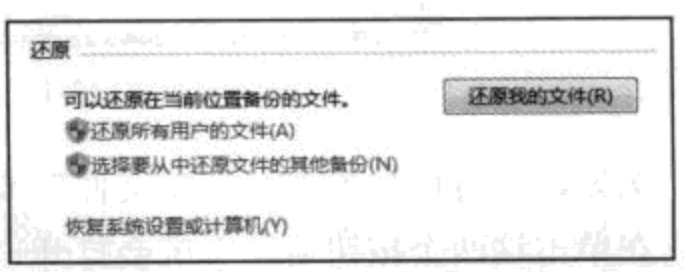


图 13-10　Windows 7 提供的还原选项

- **还原所有用户的文件** 该选项可以从备份中将所有用户的备份文件都使用最新版本进行还原。通常适用于比较重大的灾难后的还原。例如，硬盘彻底故障，更换新硬盘，并重新安装操作系统后，即可使用该选项从备份中还原所有用户的文件到最新版本。
- **选择要从中还原文件的其他备份** 该选项可供我们选择一个时间内的备份，并用于还原文件。该选项通常适合有特殊需要的时候，例如，希望将某些文件还原为某一固定时间内的版本。同时，该选项的用途与下文介绍的“以前的版本”功能非常类似。
- **恢复系统设置或计算机** 该选项还原的不是具体的文件，而是整个系统的备份。因此，该选项适合用于系统出现重大故障后的恢复，下文将介绍详细使用方式。
- **还原我的文件** 该选项只能用于还原当前用户的文件，并且只能还原到备份中包含的最新版本。

假设我们只需要还原按照上文介绍的方法备份的所有用户的库文件夹，但为了更好地演示这一程序的功能，下文并不使用最新的备份进行还原，而是打算选择一个备份来还原。因此，可以直接单击“选择要从中还原文件的其他备份”链接。

STEP 02 随后系统会对备份设备进行扫描，找到所有可用的备份，并显示在类似图 13-11 所示的界面中。在这里请留意每个备份的“计算机”，因为同一个备份介质可用于保存来自多台计算机的备份，因此，一定要确保选择了本机所需的备份。接着通过“备份期”确定自己要使用的备份，单击将其选中，然后单击“下一步”按钮。

STEP 03 随后会看到图 13-12 所示的界面，如果需要将备份中所有的内容全部还原，可以直接选中“选择此备份中的所有文件”选项，然后单击“下一步”按钮。如果只是希望还原指定的某些文件，则需要使用右侧的按钮选择要还原的内容。

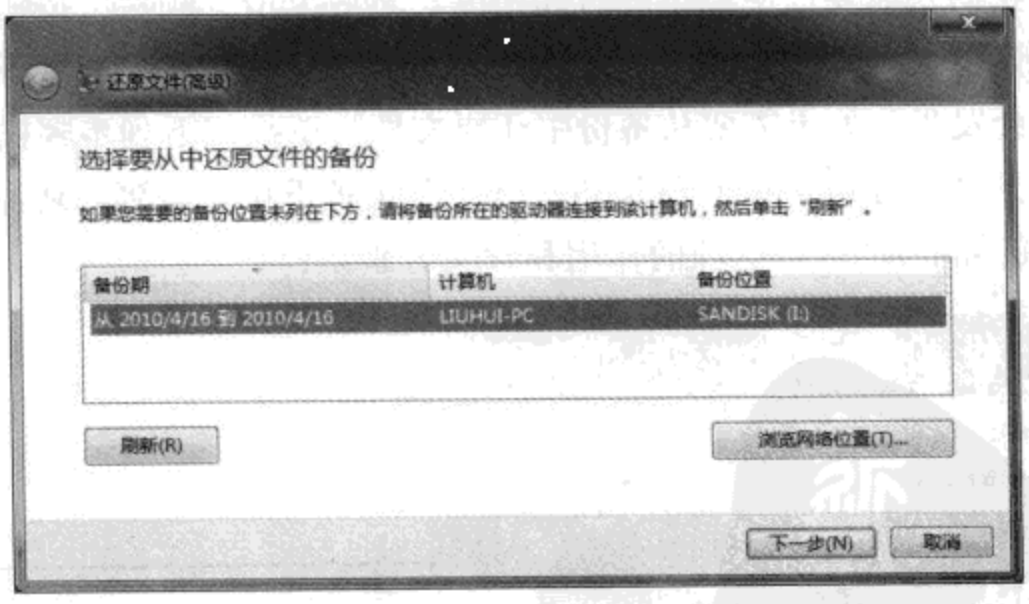


图 13-11 选择要使用的备份

例如，此时可以单击“浏览文件”或“浏览文件夹”按钮，选择要还原的文件或文件夹。在单击这两个按钮后，系统会打开一个“浏览”对话框，允许我们像浏览本地硬盘上的文件或文件夹那样浏览备份中的文件夹，我们只要找到需要还原的目标，将其选中，然

后单击“添加”按钮即可。如果不知道自己要还原的文件保存在什么位置，还可以单击“搜索”按钮，并通过文件的名称进行查找。

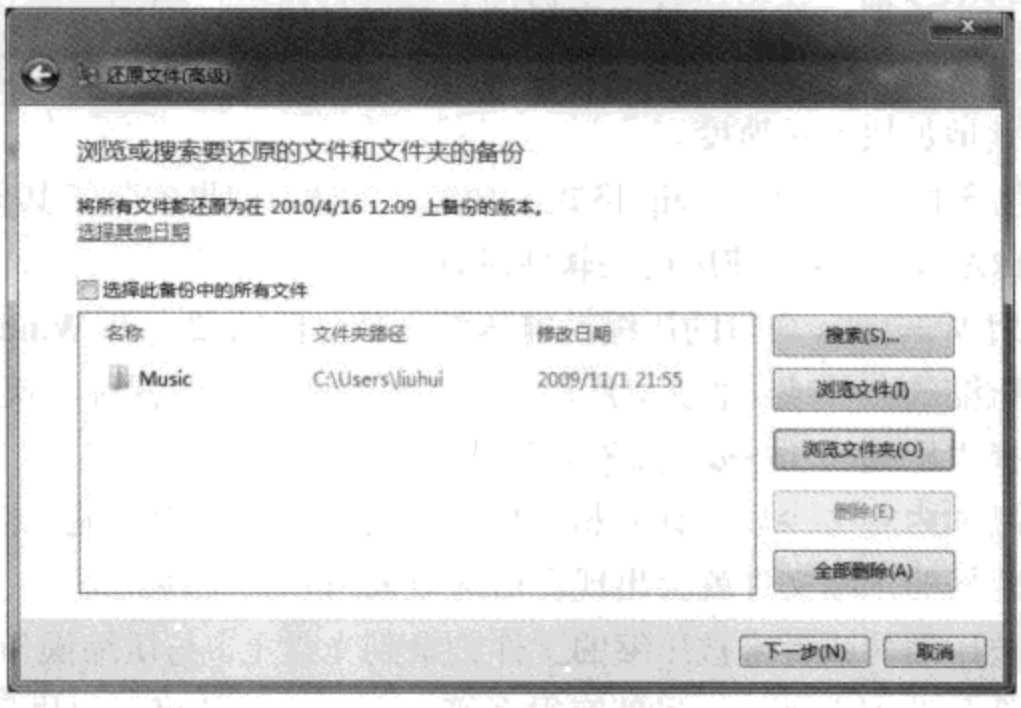


图 13-12　选择要还原的具体内容

STEP 04 添加好所有要还原的内容后，单击“下一步”按钮，随后可以看到图 13-13 所示的界面，在这里可以选择文件被还原到的位置。

如果希望用还原的文件替换原位置的同名文件，请选择“在原始位置”选项。否则请选择“在以下位置”选项，并通过“浏览”按钮选择一个新的位置。如果选中“将文件还原到它们的原始子文件夹”选项，那么被还原的文件将保持原始的树形结构。

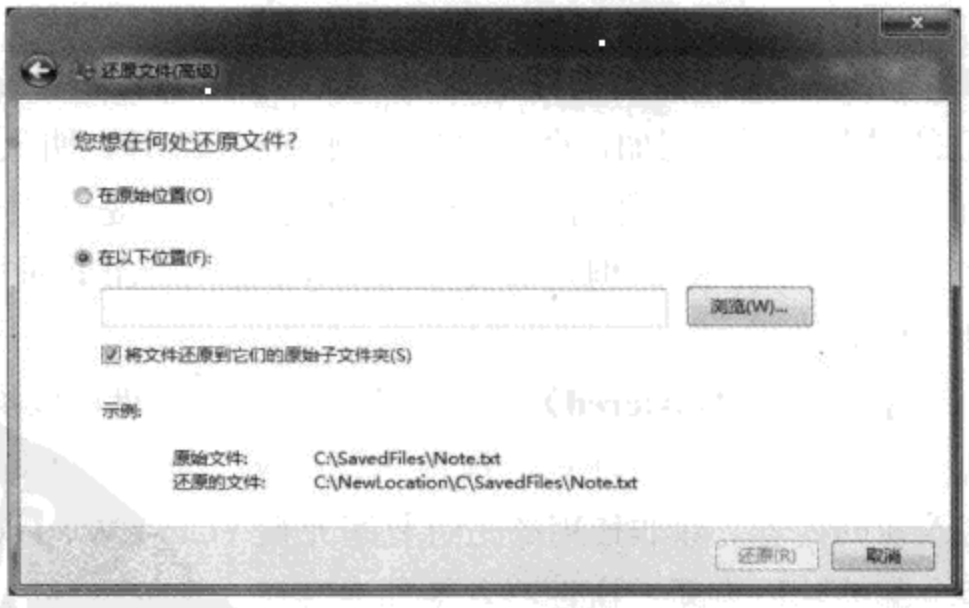


图 13-13　选择文件被还原到的位置

STEP 05 设置好所有的选项后，单击“还原”按钮，即可开始还原过程。

13.1.2.2　备份和还原不需要频繁变动的文件

对于不需要频繁变动，而且很少访问的文件，备份它只是为了存档而保留，例如，公

司前年或者去年的工作文档，可以直接将其刻录到光盘上保存。同时为了避免光盘损坏导致文件无法读取，还可以将同样的文件刻录到多张光盘上。

在刻录到光盘上之前，还可以将要备份的文件进行压缩。因为压缩可以进一步减小备份文件的体积，节约备份介质的空间。尤其是对于要备份的数量很多、很零散的小文件，压缩后还可以有效地加快刻录速度。

Windows 7 包含将文件压缩为.zip 格式的功能。当然，如果安装了其他压缩软件，例如 WinZip 或者 WinRAR，也可以使用这些软件进行压缩。

如果需要使用 Windows 自带的压缩功能压缩文件，只需要打开 Windows 资源管理器，并选中所有需要压缩的文件或文件夹，然后在选中的对象上单击鼠标右键，指向“发送到”，从弹出菜单中选择“压缩（zipped）文件夹”选项即可。

取决于要压缩的内容多少以及计算机的硬件速度，这个过程可能会需要一定的时间。压缩完成后，创建好的压缩文件就会出现在所选对象所在的文件夹下。

接着可以将被压缩的或者未被压缩的文件刻录到光盘上。与压缩操作类似，Windows 7 本身就可以将文件刻录到光盘上，虽然有很多第三方刻录软件可以提供更多的功能，不过单纯对于本例中的情况来说，Windows 自带的刻录功能已经足够。Windows 7 中的刻录功能相对来说使用更加简单。完整的刻录过程如下：

STEP 01 将刻录盘放入刻录机中，然后打开“计算机”窗口，并双击代表刻录机的盘符，随后可以看到图 13-14 所示的界面。

STEP 02 首先需要在“光盘标题”文本框中为这张光盘设定一个有意义的名字，例如光盘中的内容，或者光盘的创建时间等，随后需要选择光盘使用的文件系统，可选的文件系统如下：

- **类似于 USB 闪存驱动器（实时文件系统）** 如果选择该文件系统，则可以将光盘当做类似 U 盘的设备使用，例如，今天向里面刻录一些文件，明天再向里面刻录更多的文件，而且刻录进去的文件可以被删除（哪怕使用的是一次写入性光盘，例如 CD-R、DVD-R 或 DVD+R）。但是需要注意，Windows XP 以前的 Windows 系统无法兼容这种文件系统。
- **带有 CD/DVD 播放器（Mastered）** 如果希望刻录的光盘可以被任何计算机读取，那么可以选择这种文件系统。注意，这种文件系统必须一次性写入，一旦写入，将无法继续写入新的内容。除非使用的是可复写光盘（CD-RW、DVD±RW），可以在将光盘内容全部擦除后重新一次性写入新的内容。

选择好要使用的文件系统后，单击“下一步”按钮。

STEP 03 随后系统会对刻录盘进行初始化工作（可以将这个过程理解为对硬盘分区进行的格式化操作），初始化完成后，Windows 资源管理器会自动打开光盘的根目录。我们只需要将要刻录的文件拖动到这个资源管理器窗口中即可，其余的步骤则取决于在初始化之前选择的文件系统。

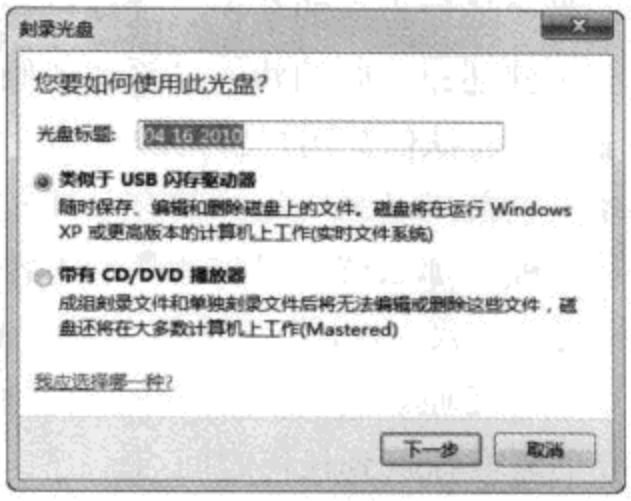


图 13-14　选择光盘使用的文件系统

STEP 04 如果选择了实时文件系统，每当将文件拖动到 Windows 资源管理器代表刻录机的窗口后，文件会被立刻刻录到光盘上（这一步类似于复制操作，而不是移动操作，拖动到光盘上的文件依然会保存在原来的位置下），我们可以依次将所有需要刻录的文件拖动过去，等到所有想要刻录的文件都拖动进入，并且已经完成刻录后，按下光驱上的退盘按钮，系统会自动对光盘进行封口（关闭轨道）。这样，如果这张光盘还没有被写满，我们还可以再次将光盘放入刻录机，并继续将更多的文件拖放进去。

需要注意，每次对光盘进行封口都会令光盘的可用容量有所损失，因此，封口的操作不要进行得太多，否则就不划算了。

STEP 05 如果选择了 Mastered 文件系统，那么当将文件拖动到刻录机的窗口中后，文件会被自动复制到系统盘下的临时文件夹中（如果要刻录的是 DVD 光盘，请首先确保系统盘具有至少 5GB 的可用空间，以免临时空间不足导致刻录失败），而不会被立刻复制到光盘上。必须一次性将所有需要复制的文件都拖动到刻录机的窗口中，然后单击工具栏上的“刻录到光盘”按钮，这时候刻录工作才会开始进行。

将要备份的文件刻录到光盘上之后，请妥善保存光盘。通常来说，光盘不能保存在太热或者太潮湿的环境下，而且最好竖起来放置，不要一堆光盘摞起来保存。另外，光盘上尽量不要粘贴标签或者用较硬的笔写字，如果需要写字，请尽量使用笔尖较软的水性记号笔或者专用的光盘笔。市面上有光盘包出售，但建议尽量不要将光盘放置在这些光盘包中保存，因为这类光盘包绝大部分的设计都不够合理，装满后，将包的拉链拉起来会导致光盘和光盘包的封套之间互相挤压，不仅容易导致光盘变形、碎裂，而且劣质光盘包会导致和光盘粘连，造成损坏。用于备份重要文件的光盘，最好选择具有独立光盘盒的优质产品。

13.1.3　使用卷影副本功能

卷影副本功能对办公用户可能更有用。简单地说，它就像一个时间机器，可以随时将我们的重要文件还原为以前的版本。

Windows 7 包含系统还原功能，可以在系统配置发生较大变化的时候自动对产生变化

的内容进行记录，创建一种叫做“还原点”的备份。这样日后如果有必要，就可以使用还原点将整个系统的配置还原到创建还原点时的状态。系统还原功能只能备份和还原操作系统，以及应用程序的状态和配置，无法保护用户自己的文档。

而以前的版本（卷影副本）功能则是系统还原的有效补充，该功能专门用于监控对用户文档的变动，一旦文档有所改变，那么就可以将改变的内容保存起来，供我们在需要的时候还原。该功能虽然和系统还原不太一样，不过确实是完全依托于系统还原功能实现的。也就是说，在（手工或自动）创建还原点的时候，系统会同时对受保护的用户文档变动内容创建备份，并供我们在需要的时候恢复到任何时间点。

很多人可能会以为该功能会大量耗费硬盘空间，其实并不是这样的。因为以前的版本功能保存的只是文档中发生改变的内容，而非整个文档，例如，假设编辑了一个 2MB 的 Word 文档，在里面添加了两个字的内容，那么在创建还原点的时候，只有这两个字的内容会被记录下来。因此，就算保存了多个版本的文档历史内容，也不会占用过多的硬盘空间。

很多人可能会问，既然可以使用备份程序备份自己的文档，那么在需要还原老版本文档的时候，为什么不直接从备份中还原？而要使用这个功能，尤其是这个功能必须启用系统还原，是否会让系统的运行速度变慢？

其实，相对备份和还原程序来说，这个功能的使用相当简单，只要单击鼠标按键就可以把文件还原为需要的任何版本。但因为系统可以用于保存还原点的硬盘空间有限制，因此，还原点不会存留很长时间，而一旦一个老的还原点被清除，对应的文档历史记录也会被清除。因此，该功能只适合需要将文档还原为近期版本的人。如果需要将文档还原为比较早的版本，例如上个月，甚至去年，那么就只能从备份中还原（前提是还保留有当时的备份文件）。

如果要使用该功能，首先必须确定自己需要保护的文档都在哪里。因为该功能依托于系统还原功能，而默认情况下，只有系统盘才被 Windows 启用卷影副本，因此，如果重要文档都保存在非系统盘，首先需要启用目标分区（该功能只能针对某一具体的本地硬盘分区启用，无法只针对特定的文件夹启用）。方法如下：

STEP 01 在“计算机”上单击鼠标右键，选择“属性”，打开“系统属性”窗口。

STEP 02 单击窗口左侧任务列表中的“系统保护”链接，随后可以打开“系统属性”对话框的“系统保护”选项卡。

STEP 03 选中要保护的文档所在的硬盘分区，然后单击“配置”按钮，随后将看到图 13-15 所示的界面。

STEP 04 对于每个分区，可以启用两种不同的保护，如果希望同时启用系统还原和卷影副本功能，需要选择“还原系统设置和以前版本的文件”选项，该选项适合用于同时安装了系统和保存了用户文件的分区。如果只希望启用卷影副本功能，可以选择“仅还原以前版本的文件”选项，该选项适合只保存了用户文件，但没有安装操作系统的分区。

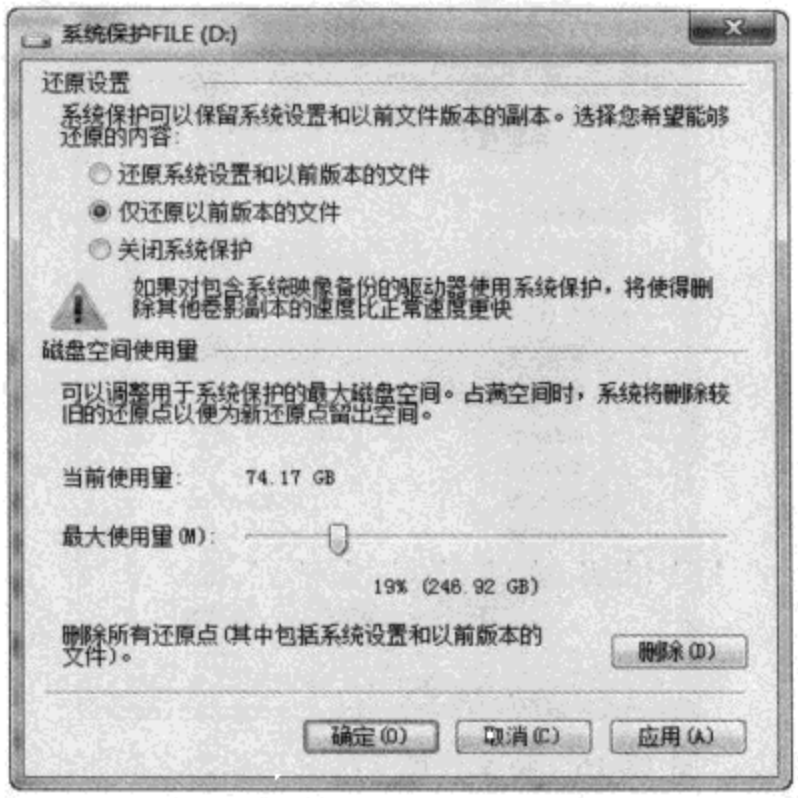


图 13-15　针对不同分区启用不同的保护

STEP 05 随后还需要设置允许该功能占用的硬盘空间数量，为此，可以根据情况拖动对话框下方的滑块（这里设置的是可被保护功能使用的硬盘空间的最大数量，并且空间是动态分配的，并不是说设置好之后，若干数量的空间就会被立刻占用）。设置完毕后，单击“确定”按钮即可。

在对其他分区启用卷影副本功能后，每次创建还原点的时候，系统都将把内容被改动的文档记录下来，供我们随时还原。通常来说，当系统符合下列条件的时候会创建还原点：

- 手工操作创建还原点。
- 系统每运行 24 小时后。
- 安装应用程序或设备驱动。
- 系统配置发生其他重大的变动。

从上面这些条件可以知道，如果系统本身没有太大变动，例如，配置好的系统，只需要使用，不需要安装新的软硬件，那么，通常来说，系统还原功能会以天为单位创建还原点，这也就意味着在正常情况下，我们至少可以以天为单位将被保护的文档还原为老版本。如果觉得这样的间隔太久，希望以更频繁的间隔创建还原点，也可以手工创建还原点。但是要注意，每个还原点间隔的频率最好不要过于频繁，因为创建大量的还原点很容易由于预先分配的硬盘空间不足而导致老的还原点被清除。

在配置好系统还原功能后，到底该怎样使用以前的版本功能呢？使用 Windows 资源管理器进入到受保护文件所在的文件夹，然后在文件或文件夹的图标上单击鼠标右键，选择“还原以前的版本”，随后可以看到图 13-16 所示的界面。

图 13-16　将文件或文件夹还原为老版本

在图 13-16 所示的界面中列出了可以通过还原点找到的所有版本，同时可以看到每个版本的修改日期。如果想要查看一个版本的内容，以便判断是不是自己需要的，可以单击将其选中，然后单击“打开”按钮，这样系统会自动将所选的版本复制到临时文件夹中，并调用相应的程序打开供我们查看。

如果发现这个版本就是需要的，可以通过“复制”按钮将该版本复制到其他位置；或者可以单击“还原”按钮，用选中的版本替换该文件当前的版本。

窍门　使用卷影副本功能恢复误删除的文件

上文曾经介绍过使用专门的反删除软件将误删除的文件恢复出来的方法。实际上，如果被误删除的文件所在分区启用了卷影副本功能，借助这一功能也可以将文件找回。为此，只需要对该文件的父文件夹使用卷影副本功能即可。例如，删除了“d:\我的文档\文件.doc”文件，就可以对“我的文档”文件夹单击鼠标右键，选择“还原以前的版本”，寻找最新的一个卷影副本，单击“复制”按钮将其内容恢复到另外一个位置，并从新位置下将“文件.doc”文件找回。

13.1.4　为文件进行异地备份

通过上文介绍的方法，我们已经可以使用 Windows 自带的工具对文件进行备份和还原。然而有时候仅仅这样做还是不够的。虽然通过使用可移动存储设备，可以将备份保存在更加安全的位置，不过一旦发生某些比较重大的自然灾害，这些备份设备也有可能受到损坏，导致文件丢失。

因此，更加稳妥的办法是进行真正的异地备份，并将备份保存在网络中。实际上，在

对数据安全性要求比较高的场合，类似的备份机制早就已经存在，但对于普通用户来说，要进行这样的备份，无论是在技术上还是成本上都不太现实。

不过现在云计算概念风头正劲，再加上宽带网络的逐渐普及，这种高级备份技术也开始逐渐走入普通人的视线。微软提供了一个名为 Windows Live Mesh（下文简称为 Mesh）的免费云存储服务，可以为每位用户提供 5 GB 的网络存储空间，用户可以使用计算机或其他电子设备向自己的 Mesh 中写入或读出文件。

例如，我们可以将一个本地文件夹（例如“文档”文件夹）添加到 Mesh 的云网络中，这样该文件夹的内容就会完全同步到 Mesh 云中，而我们在本地对其中的文件进行的任何修改，都可以自动同步出去。而且更强大的是，我们可以在两台电脑上创建一个文件夹，然后加入到同一个 Mesh 中，这样，数据就可以直接在两台电脑之间保持同步。

> **注意**　Windows Live Mesh 服务目前还处于测试阶段，尚未正式发布，因此，客户端软件以及网页都只有英文版。不过该服务的使用非常简单，并且稳定性和传输速度都比较令人满意。

限于篇幅，本书只打算介绍通过 Mesh 实现的文件异地备份。要使用这一功能，需要拥有一个 Windows Live ID，并且有可联网的计算机。随后请访问 http://www.mesh.com，单击该网页右上角的“Sign In”链接，使用自己的 Live ID 登录，随后可以看到图 13-17 所示的界面。

在图 13-17 中，首先在上方的椭圆形圆圈中单击“Add Device”（添加设备）按钮，从下方的下拉菜单中选择需要的版本（Windows 版的 Mesh 客户端软件可支持 Windows XP 以上的操作系统，虽然列表中暂时未列出 Windows 7，但实际上这个客户端是可以用于 Windows 7 的。因此，只要根据处理器架构选择 32 位或 64 位版本下载即可），并单击“Install”（安装）按钮。随后会出现文件下载对话框，这里下载的是 Mesh 客户端软件，请根据需要选择保存后运行或直接运行。

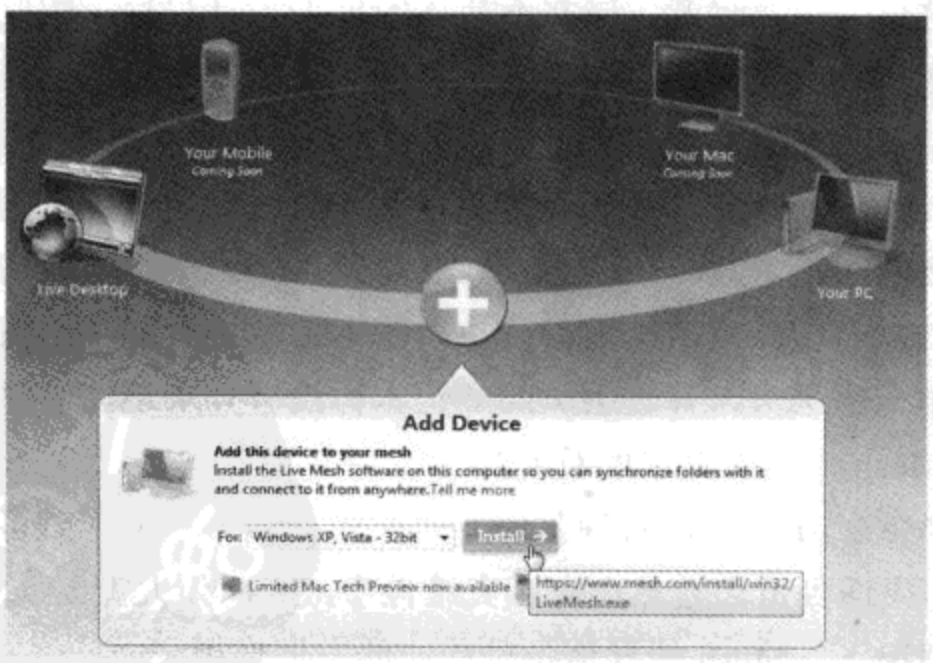


图 13-17　添加设备，并安装客户端软件

该软件的安装非常简单，大部分过程都可以自动完成。注意，在安装过程中，这个软件并不像其他软件一样显示安装界面，而仅仅是在桌面右下角显示提示对话框。取决于网络速度，整个过程可能需要一定的时间，安装完毕后，需要使用自己的 Live ID 登录。在图 13-18 所示的登录界面上输入自己的 Live ID 和密码，并通过下方的选项决定是否记住密码。其中，“Remember me”可记住 Windows Live ID，“Remember my password”可记住密码，而“Sign me in automatically”可以设置自动登录。对于只有一个人使用的 Windows 账户，建议这三个选项全部选中，随后单击“Sign in”按钮。

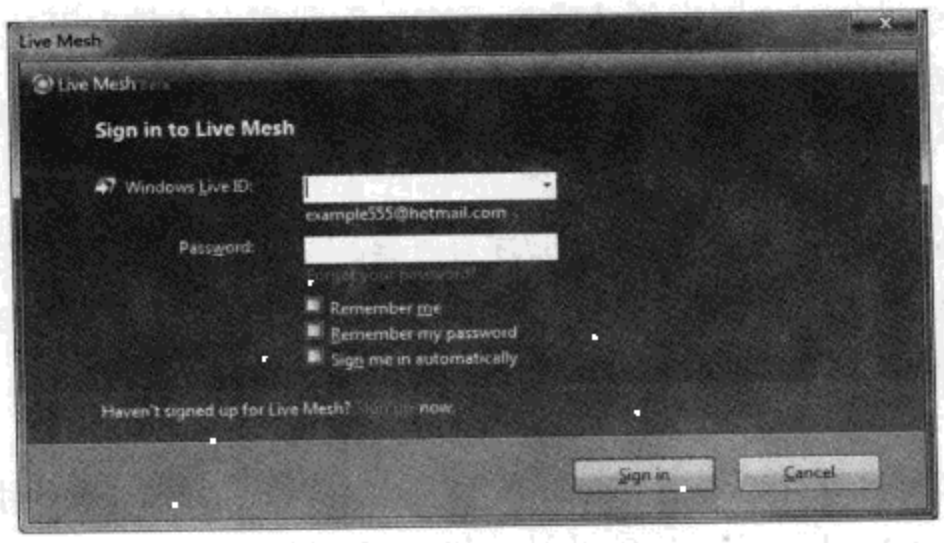


图 13-18　使用 Live ID 登录

登录成功后还会出现一个新的对话框，在这里可以为这台计算机起名，随后这台计算机就会用这里输入的名称出现在 Mesh 中。默认情况下，软件会使用 Windows 中设置的计算机名称作为名称，如果有必要，可以直接输入新的名称。其他选项保持默认设置，并单击“Add device”按钮。

添加好设备后，可以在 Mesh 网站上看到新添加的计算机，以及一个“Live Desktop”。而这里的 Live Desktop 可以理解为一个容量为 5 GB 的免费网络硬盘，我们可以直接将自己的重要文件备份到这里。需要注意，这并不是 Mesh 的设计目标，因此，相关的功能和真正的在线备份服务相比还有很大不足。不过绝大部分在线备份服务都是需要付费的，用免费的代价换回 5 GB 的备份空间以及最基本的备份，是否值得就要看每个人的需要了。

另外要注意，Mesh 这种所谓的备份功能只能用于某些特定情况，因为正常情况下，如果修改了文件，只要网络正常，改动就会立刻上传到 Mesh 中。这种情况下，如果发现自己的改动是不必要的，希望恢复改动前的状态，基本上就不可能了。但某些时候，例如，在出差途中，笔记本电脑丢失，并且丢失的笔记本再没有登录过，此时就可以等回到公司后在其他电脑上从 Mesh 中下载自己的重要数据。

因此，建议将 Mesh 作为其他常规备份方式的候补和补充。平时可使用移动硬盘、光盘等设备备份，但如果遇到重大自然灾害或灾难性事故（例如火灾），这些备份介质很可能也会被损坏。这种情况下，Mesh 的异地备份功能就发挥作用了。

在安装好 Mesh 客户端软件，并将自己的计算机加入 Mesh 后，从 Windows 资源管理

器中找到保存了要备份文件的文件夹，在该文件夹上单击鼠标右键，选择“Add folderto Live Mesh”（将文件夹添加到 Live Mesh）命令，随后将看到图 13-19 所示的“Add Folder”（添加文件夹）对话框，请单击“Show synchronization options”（显示同步选项）按钮，打开设备列表。

“Name”一栏显示了该文件夹的原名，如果有必要，可以在这里更换名称，之后文件夹将以新的名称加入 Mesh，但该文件夹在本地硬盘上的名称并不会改变。“Location”一栏列出了该文件夹的路径，不可修改。该对话框下方的设备列表中列出了所有被加入到 Mesh 中的设备，默认情况下，这里至少有两个。以图 13-19 为例，“WINDOWS7”是本机，而 Live Desktop 就是 Mesh 中的网络存储空间。如果还有其他设备加入到这个 Mesh 中，也会显示在这里。

在每个设备右侧还有一个下拉菜单，可决定与该文件夹的同步情况，该下拉菜单包含的选项如下：

- When files are added or modified　当添加或修改了文件后，即同步给该设备。
- When files are opened　当打开文件后，即同步给该设备。
- Only files smaller than 500 KB　只同步不超过 500 KB 大小的文件。
- Only files modified in the past 30 days　只同步过去一个月内修改过的文件。
- Never with this device　不与该设备同步。

通常，如果作为自己的文件异地备份，建议将本机和 Live Desktop 的同步选项都设置为“When files are added or modified”。设置完毕后单击“OK”按钮，随后 Mesh 客户端软件就会将该文件夹中的所有文件上传到 Live Desktop。取决于文件的总大小以及网络速度，这个过程可能需要一段时间。随后在单击通知区域的 Mesh 图标后，就可以从弹出的对话框内看到有关该软件的工作状态信息，如图 13-20 所示。

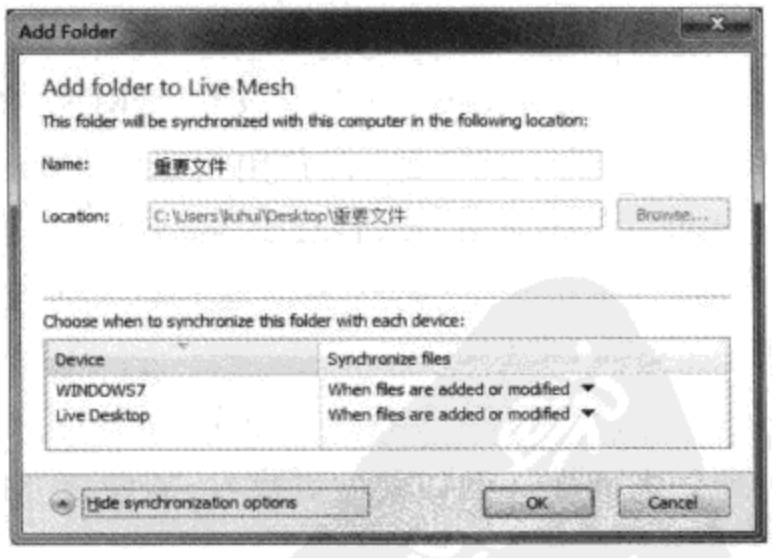


图 13-19　为文件夹设置同步选项

图 13-20　Mesh 的工作状态

在图 13-20 的底部有三个按钮，分别用于查看最近活动记录、已添加设备以及文件夹

活动。在活动记录中可以了解到 Mesh 近期发生的事件，例如，添加了新的文件夹或者对文件进行了修改或删除等操作。在设备列表中，可以看到所有加入该 Mesh 的设备以及每个设备的状态，如果该设备正在向 Mesh 上传或下载数据，则还能看到活动进度。在文件夹活动中，则可以看到目前通过 Mesh 在使用的文件夹以及每个文件夹的用户数量。

将所有重要的文件都备份到 Mesh 后，客户端软件会在后台监控对这些文件夹的访问，一旦发现有文件被修改、添加或删除，就会自动将相应的变动应用到 Mesh 中保存的文件副本上。用浏览器打开“www.mesh.com”页面，从椭圆形的设备列表中选择“Live Desktop”，随后可以看到自己的重要文件夹已经列在这里了。在这里的操作和在桌面上操作本地文件夹一样，可以用鼠标双击或右键单击文件夹并执行相关的操作，也可以在网页里打开一个类似资源管理器的窗口，直接浏览文件夹内容，如图 13-21 所示。

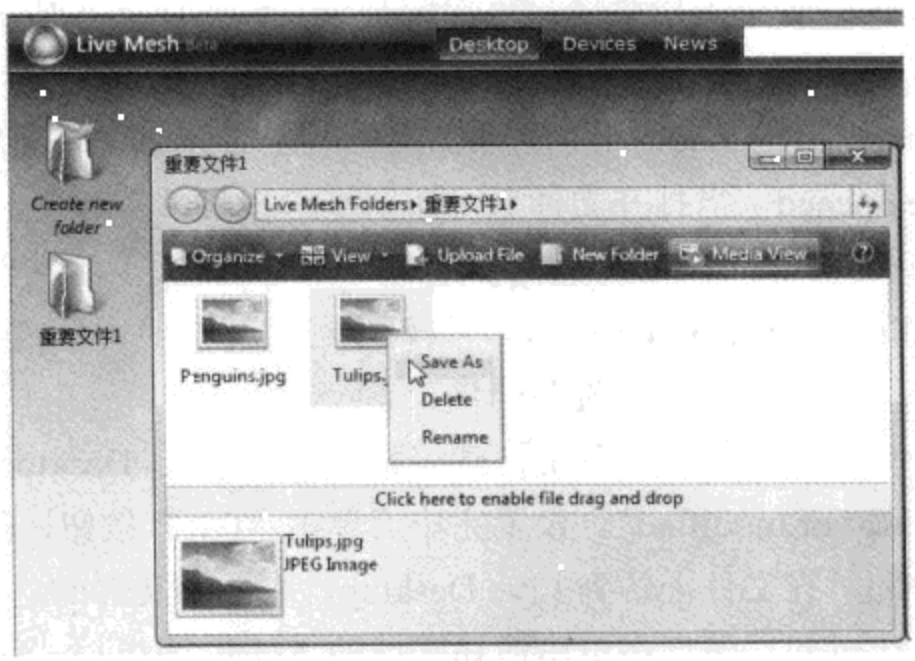


图 13-21　在网上直接查看和使用 Mesh 中的文件

如果希望将 Mesh 中的某个文件下载到本地，可以用鼠标右键单击该文件，从右键菜单中选择“Save As”（另存为）命令；也可以单击窗口底部的“Click here to enable file drag and drop”，随后需要安装一个插件。安装完成后，就可以直接用鼠标将文件在 Mesh 的网页窗口和自己的硬盘之间拖动，并进行文件传输。这样，如果在无法使用自己的计算机，需要从别人的计算机上下载某个重要文件时，就可以通过网页登录自己的 Mesh，然后将文件直接下载。也可以单击“Upload File”按钮，将其他计算机上的文件传输到自己的 Mesh 中，随后这些文件也将自动传输到自己计算机上的文件夹内。

既然这里是将 Mesh 用做备份软件，那么在出现问题时，如何进行恢复？上文介绍的“另存为”方法只适合少量文件的恢复。如果遇到大问题（例如硬盘更换），需要将 Mesh 中所有的文件夹都恢复到新硬盘上，又该怎样做呢？

其实也很简单，在解决了计算机的硬件问题后，首先安装所有必要的软件（例如 Windows 和 Mesh 客户端软件），并使用同一个 Live ID 登录。随后只要按照上文介绍的方法将新系统加入 Mesh 中，打开 Live Desktop，用鼠标右键单击想要恢复的文件夹，从右键

菜单中选择“Change sync settings”（更改同步设置）命令，随后可以打开类似图 13-19 所示的对话框，并且新系统也会列在里面。只要针对这一新的系统选择“When files are added or modified”选项即可，随后该文件夹的内容就会自动下载到新系统的用户桌面上。

如果希望将文件恢复到桌面之外的其他位置，方法也很简单。例如，假设希望将 Mesh 中的“重要文件 1”文件夹恢复到 D 盘根目录，只要在 D 盘首先创建一个“重要文件 1”文件夹，用鼠标右键单击，选择“Add folder to Live Mesh”，随后程序就会提示我们在 Live Desktop 中已经有一个名为“重要文件 1”的文件夹，并询问我们是否合并。这时候只要选择“是”，Mesh 客户端软件就会自动进行文件夹的合并和同步工作，由于 D 盘中的这个文件夹是空的，最终的结果就是，Mesh 下的“重要文件 1”文件夹的内容全部被复制到了 D 盘下的这个同名文件夹中。

13.2　系统的备份和还原

除了对重要文件进行备份外，还可以考虑将整个系统备份起来。例如，在安装好操作系统、应用程序，并给所有的软件都安装了最新的补丁程序，将系统的选项按照自己的使用习惯进行调整后，我们可以对整个系统和程序进行一次备份。这样，日后一旦系统出现故障，就可以使用备份进行还原，以免浪费时间重新安装系统和程序。

以前，如果想要对整个系统进行备份或还原，必须使用其他第三方工具软件，例如，很多人常用的 Symantec Ghost，这类软件通常都需要付费购买，而且很少有中文版，对于一般用户来说，使用上存在一定的难度。

在 Windows 7 中的情况就好多了，Windows 7 的备份功能还可对整个系统盘创建完整的备份，这样一旦系统遇到问题，无法正常使用时，即可使用之前的备份进行恢复。不仅如此，在 Windows 7 中，我们还可以使用该功能创建系统恢复光盘。这样，就算硬盘彻底损坏，在更换硬盘后，也可以使用这样的光盘启动计算机，并将系统恢复到新硬盘上。

13.2.1　系统的备份

Windows 7 在备份系统时，可以将备份保存到本地硬盘或可移动存储设备中。而需要进行恢复时，只需要用 Windows 安装光盘引导计算机，随后即可进行恢复。

假设已经安装好了 Windows 系统及其他常用软件，并结合自己的实际需要修改了必要的配置，随后即可对整个系统进行备份，此时可以按照下列步骤操作：

STEP 01　打开“开始”菜单，依次打开“所有程序”→“维护”→“备份和还原中心”，随后可以看到备份和还原主界面。

STEP 02　直接单击窗口左侧的“创建系统映象”按钮，稍等片刻后，可以看到图 13-22 所示的“创建系统映象”窗口。

STEP 03　在这里可以根据实际情况进行选择，例如，可以将备份文件保存到非系统盘

的其他本地硬盘分区、移动硬盘、大容量 U 盘或者 CD、DVD 刻录光盘上。选择好保存位置后单击“下一步”按钮，随后可以看到图 13-23 所示的确认页面。

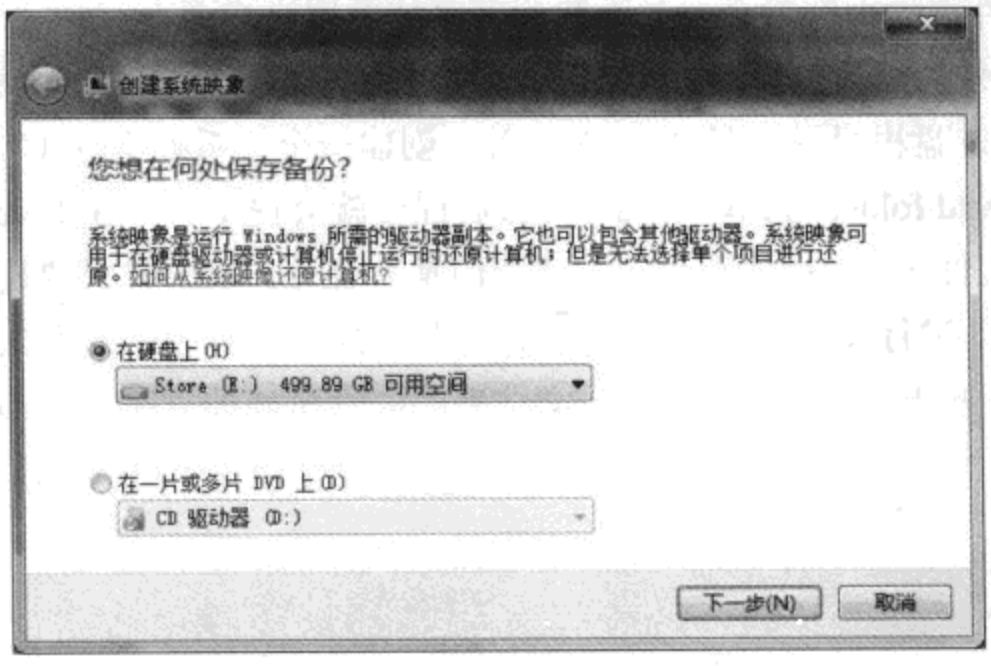


图 13-22　选择系统映象的保存位置

图 13-23　确认要备份的内容

STEP 04 在窗口上半部分的“备份位置”选项下，可以看到备份文件的保存位置，以及预计需要的存储空间数量（实际上，这个需要的存储空间数量只是估计值，因为压缩的关系，实际需要的空间数可能会少很多，但最好预先准备好足够的空间，以免备份失败）。在窗口下方的“将备份下列磁盘”内容中，可以看到将要被备份的分区。通常，如果系统中包含多个重要分区，那么所有这些分区都会被备份。例如，如果将 Windows 安装到 D 盘，实际上因为 C 盘保存了引导文件，因此，C 盘和 D 盘都将被自动备份。

STEP 05 如果觉得可以开始，单击“开始备份”按钮即可。取决于要备份的文件数量，以及计算机硬件的性能，备份可能需要一段时间。备份完成后单击“关闭”按钮即可。

窍门　节约硬盘空间

在开始对整机进行备份之前，建议先对硬盘进行清理，删除不需要的垃圾文件，以便加快备份的速度，并减少需要的存储空间数量。请打开“计算机”窗口，然后在代表 Windows 安装分区的硬盘分区图标上单击鼠标右键，选择“属性”，在随后出现的“属性”对话框的“常规”选项卡上单击“磁盘清理”，等待片刻，并单击“清理系统文件”按钮，随后即可看到图 13-24 所示的“磁盘清理”对话框。在该对话框中，首先打开“其他选项”选项卡，单击程序和功能，以及系统还原和卷影复制选项下的“清理”按钮，并单击“删除”按钮以确认。然后回到“磁盘清理”对话框，选中要删除的垃圾文件类型，然后单击“确定”按钮，在随后出现的对话框中单击“删除文件”按钮加以确认。

这里需要注意，对于“缩略图”内容，可根据实际需要决定是否要清理。通过使用缩略图功能，在 Windows 资源管理器中进入包含大量多媒体内容（图片、视频等）的文件夹后，

可以快速显示媒体的缩略图。如果将缩略图全部清理掉，下次进入这样的文件夹时依然会重新创建缩略图缓存，并且文件的显示速度将受到影响。

图 13-24　清理不需要的垃圾文件

备份完毕后，如果备份工具检测到系统安装有光盘刻录机，还会询问是否创建修复光盘。此时请根据实际情况决定，通常建议保留一份系统修复光盘，因为硬盘出故障的可能性也非常大，尤其是笔记本计算机，很可能因为振动或其他原因导致硬盘故障。因此，通过使用系统修复光盘，只需要更换故障的硬盘，并使用这样的光盘引导计算机，即可将整个系统连同安装的所有软件（前提是这些软件也被安装在系统盘）都恢复为备份时的状态。

如果打算创建系统修复光盘，只需要单击“是”，并在刻录机中放入空白的 CD/DVD 刻录盘，然后单击“创建光盘”按钮即可。这里需要注意，如果备份文件的体积太大，一张光盘容纳不下，备份工具还可以将内容进行拆分，并分别刻录到多张光盘上，但这就需要对光盘创建好编号，并在需要修复系统的时候按顺序使用每张光盘。

13.2.2　灾难后的还原

在系统出现重大故障，需要还原到刚安装好的状态时，就可以使用按照上文步骤创建的系统映象备份。下面将介绍使用本地硬盘上保存的映象进行修复的方法，如果创建了系统修复光盘，其方法也类似，不过会更简单一些。使用硬盘上保存的映象进行修复的操作步骤如下：

STEP 01　准备好 Windows 7 安装光盘，并在计算机的 BIOS 设置中设定通过光盘引导计算机（具体的设置方法请参考计算机或主板的说明书）。

STEP 02　打开计算机电源，立刻将 Windows 7 安装光盘放入计算机（对于较新的计算机或主板，可能带有临时更换引导设备顺序的功能，通常可以在开机后按下键盘上的某个按键，然后选择临时使用的引导设备，详细做法请阅读计算机或主板说明书）。

STEP 03 如果设置无误，那么计算机会自动从光盘引导，稍等片刻，屏幕上就会出现一个绿色的滚动条，就像 Windows 正常启动时那样。

STEP 04 当看到安装 Windows 对话框之后，选择要安装的语言、时间、货币格式，以及键盘和输入方法，设置好之后单击“下一步”按钮。

STEP 05 随后可以打开“安装 Windows”对话框，在这个对话框中单击左下角的“修复计算机”链接，随后安装程序会自动扫描硬盘上已经安装的 Windows（如图 13-25 所示）。因为我们需要的是从备份还原，而不是需要修复现有的 Windows，因此，直接选择“使用以前创建的系统映象还原计算机”单选框，然后单击“下一步”按钮。

STEP 06 随后可以看到图 13-26 所示的“选择系统镜象备份”对话框。如果本地硬盘，或者所选的可移动存储设备中保存了多个系统映象，默认情况下，还原工具将选择最新的备份。如果需要使用其他备份，则可以选中“选择系统映象”，并单击“下一步”按钮，选择要使用的备份。这里我们直接选择最新的备份，保留默认设置，并单击“下一步”按钮。

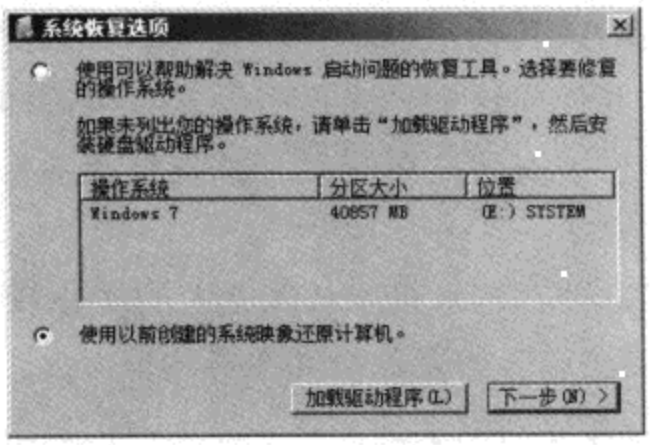


图 13-25　选择使用映象还原的选项

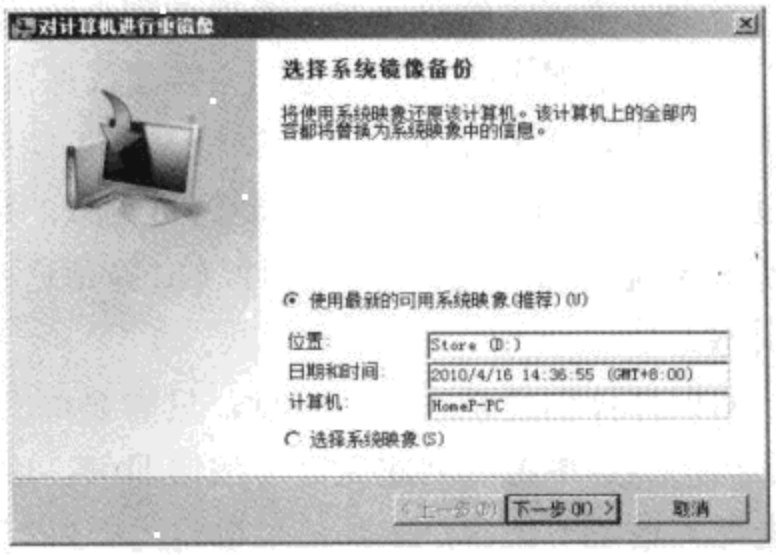


图 13-26　选择要使用的映象

STEP 07 接下来可以看到图 13-27 所示的界面，这里列出了还原时的相关选项。其中有一个“格式化并重新分区磁盘”选项比较适合通过光盘将系统的备份还原到新硬盘的情况，这样就可以让新硬盘保持与老硬盘相同的分区结构。如果是从硬盘上还原备份文件，并且是将备份还原到同一台计算机上，则没必要选择该选项。

在选中“格式化并重新分区磁盘”的选项后，还可以使用“排除磁盘”按钮指定不重新分区的磁盘。该功能适合安装有多块硬盘的计算机，例如，计算机上安装了两块硬盘，一块用于安装操作系统和应用程序，另一块用于保存用户数据。对于这种情况，可以将保存数据的硬盘排除掉，以免破坏其中保存的数据。

单击“高级”按钮后，在弹出的对话框中有两个选项可供完成还原后自动重启动计算机，以及自动对硬盘进行错误检查。我们可以根据需要选择这两个选项。

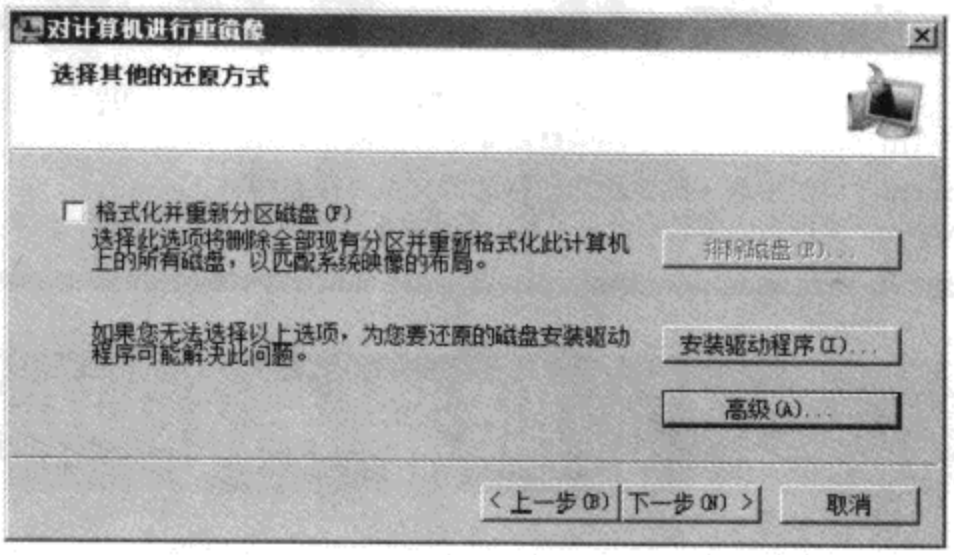


图 13-27　其他高级选项

STEP 08 设置完毕后，单击“下一步”按钮复查所有的信息，确认无误后，即可单击“完成”按钮，随后工具会自动从映象中恢复系统，这个过程可能需要一段时间。

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

Broadview®
www.broadview.com.cn

《Windows 7 安全指南》读者交流区

尊敬的读者：

感谢您选择我们出版的图书，您的支持与信任是我们持续上升的动力。为了使您能通过本书更透彻地了解相关领域，更深入的学习相关技术，我们将特别为您提供一系列后续的服务，包括：

1. 提供本书的修订和升级内容、相关配套资料；

2. 本书作者的见面会信息或网络视频的沟通活动；

3. 相关领域的培训优惠等。

请您抽出宝贵的时间将您的个人信息和需求反馈给我们，以便我们及时与您取得联系。

您可以任意选择以下三种方式与我们联系，我们都将记录和保存您的信息，并给您提供不定期的信息反馈。

1．短信

您只需编写如下短信： B11211+您的需求+您的建议

发送到1066 6666 789（本服务免费，短信资费按照相应电信运营商正常标准收取，无其他信息收费）

为保证我们对您的服务质量，如果您在发送短信24小时后，尚未收到我们的回复信息，请直接拨打电话（010）88254369。

2．电子邮件

您可以发邮件至jsj@phei.com.cn或editor@broadview.com.cn。

3．信件

您可以写信至如下地址：北京万寿路173信箱博文视点，邮编：100036。

如果您选择第2种或第3种方式，您还可以告诉我们更多有关您个人的情况，及您对本书的意见、评论等，内容可以包括：

（1）您的姓名、职业、您关注的领域、您的电话、E-mail地址或通信地址；

（2）您了解新书信息的途径、影响您购买图书的因素；

（3）您对本书的意见、您读过的同领域的图书、您还希望增加的图书、您希望参加的培训等。

如果您在后期想退出读者俱乐部，停止接收后续资讯，只需发送“B11211+退订”至10666666789即可，或者编写邮件“B11211+退订+手机号码+需退订的邮箱地址”发送至邮箱：market@broadview.com.cn 亦可取消该项服务。

同时，我们非常欢迎您为本书撰写书评，将您的切身感受变成文字与广大书友共享。我们将挑选特别优秀的作品转载在我们的网站（www.broadview.com.cn）上，或推荐至CSDN.NET等专业网站上发表，被发表的书评的作者将获得价值50元的博文视点图书奖励。

我们期待您的消息！

博文视点愿与所有爱书的人一起，共同学习，共同进步！

通信地址：北京万寿路 173 信箱　博文视点（100036）　　电话：010-51260888

E-mail：jsj@phei.com.cn，editor@broadview.com.cn

www.phei.com.cn
www.broadview.com.cn

- android与iphone及ipad开发书籍 ----------持续不断更新中.....
- c、c++、c#语言pdf书籍及vip视频教程 c、c++、c#、vc等-------持续不断更新中.....
- delphi《书籍》及《视频》教程 ----------持续不断更新中.....
- E网情深VIP系列视频教程 黑客破解菜鸟修练班，VB编程学习班，仿站学习培训，免杀培训，个人系统攻防系列教程，服务器搭建学习班，PHOTOSHOP平面设计班，基础制作论坛（论坛网站搭建），网赚系列教程，网站建设教程，网站漏洞基础，远程控制教程，软件破解班，脚本漏洞提权班
- IT9网络学院VIP系列视频教程 免杀培训班，VMware虚拟机，零基础学习C语言，网游外挂开发精品系列语音教程（外挂教程学习必备研修31课全），VB语言教程30课全，Delphi编程到精通，远程控制软件，加密解密班，网络安全与黑客攻防培训，从入门到精通完整系统化学习C++编程，从入门到精通零基础学习汇编，wordpress教程(个人博客系统49课全)，外行人做易语言盗号和钓鱼程序语音教程 网址：WLSAM168.400GB.COM
- Java书籍 ----------持续不断更新中.....
- photoshop、CorelDRAW、AutocAD等图像处理书籍及vip视频教程 -------持续不断更新中.....
- powerbuilder书籍大全
- Visual Basic语言vip视频教程及pdf书籍 ----------持续不断更新中.....
- windows、linux系统开发、系统封装等pdf书籍及VIP视频教程 ----------持续不断更新中.....
- 《3DS Max》pdf书籍
- 《汇编语言》、《反汇编》及《调试》pdf书籍及vip视频教程 ----------持续不断更新中.....
- 《电子书、电子书、还是电子书》pdf专题库 编程开发，家居美食，儿童益智，人物传记，增强记忆，快速阅读
- 信息系统项目管理师、网络工程师、系统分析师等软考类书籍
- 华中红客系列vip视频教程 脚本攻防培训班，源码免杀培训班，Css语言培训班，C语言，Dreamweaver网页设计，html网页设计培训班，PC安全班， php脚本语言培训班，VMWare虚拟机专题，webshell提权培训班，防站教程，零基础免杀培训班，刷钻速成班，脱壳破解班，外挂编写班，网络赚钱培训班，网站入侵培训班
- 外挂、驱动、逆向及封包视频教程 郁金香、独立团、夜猫论坛、天都吧、看流星论坛、一切从零开始等等
- 安全中国系列vip视频教程 易语言软件编程培训班，ASP.net网站开发项目实战培训班
- 我的收藏
- 按键精灵及TC脚本开发软件视频教程 ----------持续不断更新中.....

当前位置：/《电子书、电子书、还是电子书》pdf专题库

文件名 ⇕

PDF电子书专题库，内容详尽，每天不断更新！！

- 办公类软件使用指南
- 医学
- 历史人物传记
- 哲学宗教
- 外语资料（除英语外） （除英语外）
- 官场类小说
- 建筑工程类
- 情感生活类小说
- 政治军事
- 教育学习科普大全
- 文学理论
- 智力开发、增强记忆、快速阅读技巧大全
- 社会生活
- 科学技术
- 程序编程类
- 经济管理
- 网络安全及管理
- 网赚系列
- 美食小吃烹饪煲汤大全
- 课外读物

本网盘内容太多，持续不断更新，发布各类视频教程、pdf书籍，包括破解、加解密、外挂辅助制作，易语言培训教程、编程语言、网页制作等等，教程及书籍仅用于学习,如用于商业或非法用途的后果自负！

网址：WLSAM168.400GB.COM

- VIP培训教程，易语言黑月VIP视频教程，天都网易语言系列培训教程(100集全)，集中营易语言学习视频(80集)
- 棉猴系列vip视频教程 gh0st远控控制源码讲解教程，套接字编程，DLL程序编写，键盘监听驱动程序编写，驱动基础教程，AsyncSelect模型QQ程序教程，C++语言入门基础，NB5.5源码分析教程
- 游戏开发pdf书籍 ----------持续不断更新中.....
- 炒股投资pdf书籍及视频教程 短线高手系列，短线天王系列，操盘论道系列，翻倍黑马，看盘快速入门，庄家手法大曝光等等。 网址：WLSAM168.400GB.COM
- 热门小说集中营 傲世九重天，网游之三国时代，武动乾坤
- 甲壳虫VIP教程全集 asp教程，Delphi培训班，FLASH培训班，Java培训班，linux培训班，PHP培训班，源码免杀班，甲壳虫C++，脚本功防班，免杀班初、中、高级班，破解班，源码免杀班，脱壳班，易语言培训班，无特征码免杀，网站架构培训班，外挂高级班，外挂初级班第1、2部
- 破解、免杀、入侵、脱壳、攻防及漏洞分析系列VIP视频教程（80多部） 天草、黑客动画吧等等--------持续不断更新中....
- 网站建设相关的pdf书籍及各种vip视频教程 ----------持续不断更新中.....
- 网赚、淘宝系列vip视频教程 网赚30天新人魔鬼训练，屠龙网赚团队vip课程，站长大学网赚视频（50课全），图腾团队日赚1000元竞价行销教程，屠龙团队淘宝宝贝卖疯系列，站群网赚系列，淘宝开店视频，红星挂机日赚10元，百万流量系列，漂流瓶圣手全自动挂机引，贴吧邮件定向营销疯狂成交量月入万元
- 英语学习资料百科大全 不断更新。。。
- 饭客论坛系列VIP视频教程 脚本入侵班，黑客之免杀教程，易语言教程，无线网络攻防教程，入侵教程，delphi系列教程，黑客基础入门
- 黑客书籍 有关黑客、安全、加解密技术等等----------持续不断更新中.....
- 黑手安全网VIP系列视频教程 DIV+CSS网页布局，Dreamweaver教程，flsah动画教程，photoshop教程，跟我一起学C++课程，抓鸡
- 黑鹰、黑基、黑防、黑盾vip系列视频教程 破解提高班66课全，SQL注入，ASP注入教程，完完全全学会抓肉鸡，脱壳破解教程50课全，提权班，C语言特训班26讲全，黑客脚本特训班，黑客工具特训班，dedecms仿站教程，VC编写远控30课全，网页美工特训班，木马免杀特训班，驱动开发技术VIP培训班，外挂破解等等。

- [电脑世界的通关密语：电脑编程基础].(杉浦贤).滕永红.扫描版.pdf
- [程序语言的奥妙：算法解读（四色全彩）].(杉浦贤).李克秋.扫描版.pdf
- [差错：软件错误的致命影响].(帕伯斯).邝宇恒等.扫描版.pdf
- [算法之道（第2版）].邹恒明.扫描版.pdf
- [O'Reilly：深入学习MongoDB].(霍多罗夫).巨成等.扫描版.pdf
- [深入浅出WPF].刘铁猛.扫描版.pdf
- [Go语言·云动力（云计算时代的新型编程语言）].樊虹剑.扫描版.pdf
- [精通.NET互操作：P/ Invoke、C++ Interop和COM Interop].黄际洲等.扫描版.pdf
- [编程的奥秘：.NET软件技术学习与实践].金旭亮.扫描版.pdf
- [O'Reilly：学习OpenCV（中文版）].(布拉德斯基等).于仕琪等.扫描版.pdf
- [Go语言编程].许式伟等.扫描版.pdf 网址：WLSAM168.400GB.COM
- [MySQL技术内幕：SQL编程].姜承尧.扫描版.pdf
- [Tomcat权威指南（第2版）].(布里泰恩等).吴豪等.扫描版.pdf
- [Ext江湖].大漠穷秋.扫描版.pdf
- [IT名人堂·Oracle DBA突击：帮你赢得一份DBA职位].张晓明.扫描版.pdf

Total: 77 1 2 3 4 5 6 ›

反侵权盗版声明