Broadview
www.broadview.com.cn

“十一五”国家重点图书出版规划项目

MVP 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

“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。

- 小心朋友通过 IM 软件发来的网页链接：如果朋友通过 IM 软件发来了某个网页的链接，在打开前最好先问问对方是否发送过这样的东西，因为有时候这可能是对方系统感染了病毒后自动发送的，如果直接单击这样的链接，我们的系统也有可能会中毒。
- 安装软件一定要小心：现在很多软件的安装程序中都捆绑有其他非必要的软件，这类软件一旦安装，往往很难卸载，并且可能会给系统带来很多麻烦。因此，在安装软件时一定要小心查看所有的选项，尽量不要安装来自陌生网站的软件。

其实现在很多人已经开始意识到这个问题，但关键在于，并不是每个人都能充分理解系统中不同选项对于安全性的影响。而且很多人对于目前层出不穷的新安全问题也并不了解，因此，本书的主要目的是向大家介绍这些选项，并通过实例告诉大家在网络上遇到这类问题后应该处理。

## 本书主要内容

| 第 1 部分　Windows 安全 | |
|---|---|
| 第 1 章 | 介绍如何将 Windows 的更新程序直接集成到安装文件里，以及在安装 Windows 的过程中需要注意的安全问题和安装好后需要留意的设置 |
| 第 2 章 | 介绍如何创建和管理用户账户，以及 Windows 7 中改进后的用户账户控制功能的作用 |
| 第 3 章 | 重点介绍了 Windows 中数百条的安全策略，因为通过这些策略可以改变 Windows 在安全性方面的很多选项 |
| 第 4 章 | 介绍对 Windows 系统进行更新的必要性，以及如何更好地进行更新 |
| 第 5 章 | 介绍如何利用 NTFS 文件系统的各种特性保护文件安全，同时还介绍 Office 文档的安全问题，以及文件被彻底删除和误删除后的恢复方法 |
| 第 2 部分　网络安全 | |
| 第 6 章 | 介绍使用无线 WiFi 网络时可能遇到的安全问题，以及如何避免因为这些问题受到攻击 |
| 第 7 章 | 介绍在使用局域网共享文件时需要注意的安全问题，以及如何通过共享权限和 NTFS 权限配合限制网络共享的访问 |
| 第 8 章 | 介绍 Windows 自带的 Windows 网络防火墙的使用方法 |
| 第 3 部分　病毒和恶意软件 | |
| 第 9 章 | 介绍如何在浏览网页、收发邮件、网络聊天以及安装软件的时候保护自己的系统安全 |
| 第 10 章 | 介绍如何使用反病毒软件保护自己的系统安全，以及如何防范恶意软件 |
| 第 4 部分　其他安全问题 | |
| 第 11 章 | 介绍如何使用 Windows 7 的家长控制功能对孩子使用计算机进行限制和约束 |
| 第 12 章 | 介绍如何利用 Windows 7 的 BitLocker 和 BitLocker To Go 功能保护系统不受脱机攻击 |
| 第 13 章 | 介绍如何利用系统自带的或者第三方程序备份自己的文档或整个系统，并在需要的时候进行还原 |

## 本书特色

虽然这本书名叫《Windows 7 安全指南》，然而本书并不仅仅介绍有关 Windows 本身的

安全问题，还包含了一般用户在使用 Windows 操作系统完成日常工作的过程中可能遇到的各种安全风险，以及解决和预防办法。

因此，通过阅读本书，将可以保证自己的计算机整体环境更安全、可靠。

## 读者对象

本书的目标读者是使用 Windows 操作系统进行工作或娱乐的一般用户。即使完全没有计算机技术基础，只希望使用计算机完成自己工作的人，也完全可以通过本书了解如何操作才能提高计算机的整体安全性；而对于希望“知其然，也知其所以然”的人，将可以了解到一些深入的技术细节和原理，并能通过这些信息更好地使用 Windows。

## 致谢

本书主要由刘晖、汤雷、张诚编写，其他编写人员包括刘宝良、王凤霞、董晓兰、刘步庭、李红莉、刘进业和张惠玲。本书在编写过程中得到了电子工业出版社博文视点资讯有限公司郭立总经理、李冰编辑、黄爱萍编辑等人的大力帮助，在这里对他们表示衷心的感谢，没有他们的帮忙，本书的顺利出版是不可能的。

在写这本书的时候，作者已经尽了最大的努力保证在技术和文字上没有什么错误或者疏漏，但由于水平有限，难免会出现一些错误或者不足，敬请指正。如果您在阅读本书的过程中有什么疑难问题，请发邮件到 jsj@phei.com.cn，并使用“《Windows 7 安全指南》技术问题”作为邮件主题，方便及时处理。

刘　晖

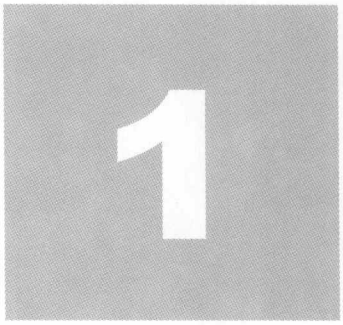
2010 年 5 月

# 目　录

## 第 1 部分　Windows 安全

# 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。

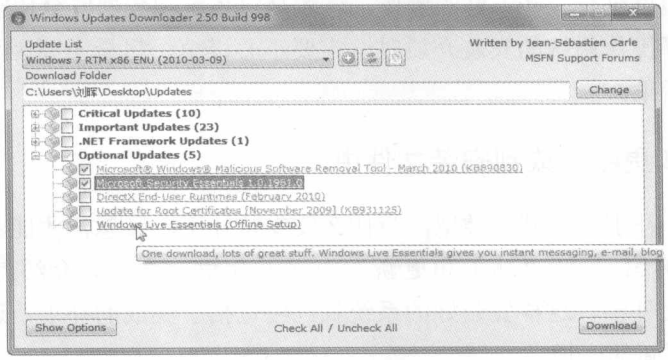



图 1-1　从列表中选择要下载的更新

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）。

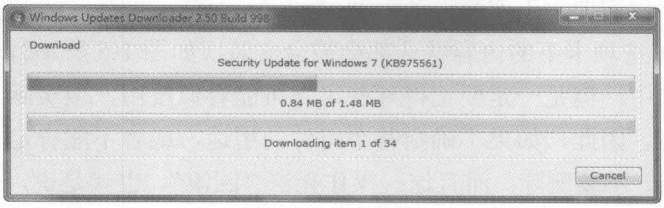



图 1-2　下载所有选中的更新

**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）。

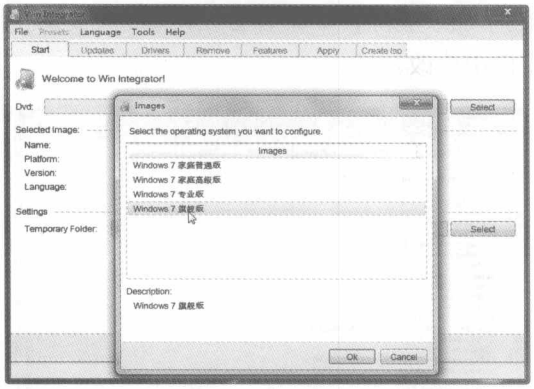



图 1-3　指定安装文件的位置并选择版本

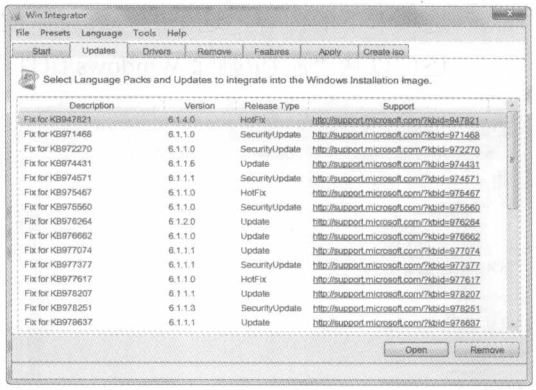



图 1-4　添加好的更新程序

**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。

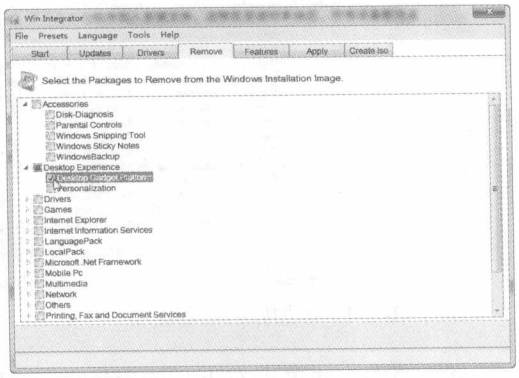



图 1-5　需要慎重增/删的组件

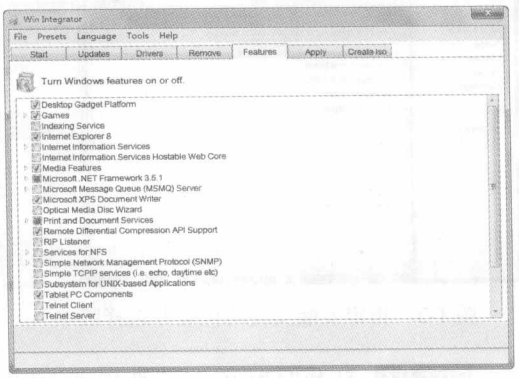



图 1-6　可以放心增/删的组件

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