Pro Internet Explorer 8 & 9 Development

IE8 & 9开发实战：基于下一代IE的应用开发

(美) Matthew Crowley 著
贾洪峰 译

Apress®
清华大学出版社

IE8 & 9 开发实战：基于下一代 IE 的应用开发

(美) Matthew Crowley 著
贾洪峰 译

清华大学出版社
北 京

Matthew Crowley
Pro Internet Explorer 8 & 9 Development
EISBN: 978-1-4302-2853-0

北京市版权局著作权合同登记号 图字：01-2010-8136

图书在版编目(CIP)数据

IE8 & 9 开发实战：基于下一代 IE 的应用开发/(美)克罗利(Crowley，M.) 著；贾洪峰 译.
—北京：清华大学出版社，2012.1
书名原文：Pro Internet Explorer 8&9 Development
ISBN 978-7-302-27358-5
Ⅰ.I… Ⅱ.①克… ②贾… Ⅲ.互联网络—浏览器 Ⅳ.TP393.409.2

中国版本图书馆 CIP 数据核字(2011)第 233009 号

责任编辑：王 军 徐燕萍
装帧设计：牛艳敏
责任校对：成凤进
责任印制：杨 艳
出版发行：清华大学出版社
http://www.tup.com.cn
社 总 机：010-62770175
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
地 址：北京清华大学学研大厦 A 座
邮 编：100084
邮 购：010-62786544
印 刷 者：清华大学印刷厂
装 订 者：三河市新茂装订有限公司
经 销：全国新华书店
开 本：185×260 **印 张**：23.75 **字 数**：578 千字
版 次：2012 年 1 月第 1 版 **印 次**：2012 年 1 月第1 次印刷
印 数：1～3000
定 价：58.00 元

产品编号：036786-01

前　言

有很多开发人员希望使用 Internet Explorer 8 和 9 来构建 Web 站点、浏览器扩展以及桌面应用程序，本书的编写旨在为他们提供坚实的技术指导。在微软 IE 工程团队工作期间(以及之前担任 Web 开发人员期间)，我就注意到关于 IE 开发过程，缺乏一些简单易懂及最新的信息。

IE 9 的发布已经使微软重新获得在线空间领域的正统性，而在此之前的将近 10 年间，微软经历了市场份额下滑、与 Web 开发社区关系恶化等问题。为了重建这种关联性，IE 就不能再是一个“后知后觉者”，也不能再是一大堆为 Web 开发人员准备的错误补丁，而应当是主流 Web 和浏览器扩展开发周期的组成部分。开发人员需要更新自己对这一浏览器的理解，特别是对 IE 9，因为它这次是作为一种现代化的主流开发平台而再度出现的。

我希望本书能够帮助读者快速、高效地掌握 IE 8 和 IE 9 编程的核心概念。利用书中提供的概念和示例，读者将会学习到如何创建和维护功能强大的浏览器、应用程序和 Web 服务软件，这些不仅能够利用微软下一代 Internet 平台的功能，还能对其进行扩展。

本书内容

本书旨在帮助开发人员创建用于扩展 IE 功能的浏览器、应用程序和 Web 服务软件。可以使读者：

- 理解 IE 的体系结构与设计
- 构建基于浏览器的扩展，如 ActiveX 控件、工具栏、浏览器栏、浏览器帮助程序对象和可插入协议
- 利用加速器、网页快讯和搜索提供程序来扩展现有 Web 服务
- 使用 IE API、COM 对象和控件来增强应用程序
- 设计与 Windows 安全功能集成在一起的扩展
- 调试为 IE 设计的应用程序
- 处理应用程序的兼容性和升级方案
- 利用功能强大的工具来改进扩展开发
- 精通构建世界级应用程序的最佳实践

本书读者对象

本书主要面向中高级开发人员。在编写本书时，假定读者已经熟悉了 HTML，JavaScript 和 CSS。后面的一些章节需要读者对 C++以及(或者)C#有一定的了解。COM/COM+编程经验在某些地方也是有用的；但这些例子都非常明了，没有这些经验也能理解。

尽管本书主要是面向那些关注代码的个人，但对 Web 社区的大多数人也是有价值的。潜在读者包括：

- 寻求开发、部署新理念的创业者

- 寻求基于 IE 开发框架开发新功能的产品规划师
- 向消费者或企业管理员推销加载项的营销员
- 关注 Web 浏览器和 Internet 编程的发烧友

本书的组织方式

IE 是一个内容丰富的应用程序平台，涵盖了云、桌面和两者之间的一切东西。尽管本书不可能全面介绍 IE API 所能触及的所有内容与精妙之处，但在不牺牲各主题必要深入性的前提下，希望能够尽可能扩展各主题的广泛性。

除第 1 章之外，本书采用由 Web 到桌面、自上而下的方法来介绍各个主题。本书的一般领域(在章节顺序上反映出来)如下：

- 浏览器体系结构(第 1 章)：这一部分介绍了 IE 平台的历史、内容和体系结构。它全面地概括了浏览器的体系结构以及它与 Web 服务、操作系统之间的交互。阅读本章后，就可以很轻松地理解后续各章介绍的主题了。
- Web 应用程序(第 2、3、5、7 章)：这几章概括介绍了 IE 平台中的 Web 改进。相关主题包括：对 HTML 和 CSS 标准的支持、DOM 的添加、Ajax 和 JSON 特性以及可访问性的改进。您将学习如何利用这一最新版本的浏览器中添加的新功能(以及跨浏览器功能)来增强 Web 应用程序。
- Web 服务扩展(第 4、8、9 章)：这一部分介绍 Web 服务交互。这一部分的各章揭示了很多方法，可以用来开发一些应用程序，在浏览器用户界面和 Web 服务之间架起沟通的桥梁。加速器、网页快讯、搜索提供程序和其他很多应用程序都将进行详细讨论。这一部分还会介绍很多高级主题和最佳实践，提供非常方便的参考指南。
- 浏览器扩展(第 10、12、13、14 章)：这几章包含了构建和部署浏览器扩展的教程，会讲解如何构建大量的扩展性服务，并与之进行交互，这些服务包括：浏览器帮助程序对象、ActiveX 控件、工具栏和浏览器栏。每一章都包含一些高级主题，以及可以经常参考的最佳实践。
- 桌面应用程序和脚本(第 11、15 章)：这两章主要介绍与浏览器平台进行交互的桌面应用程序和脚本。包括对 WebBrowser 的介绍以及编写浏览器脚本的操作方法指南。

其他资源

关于如何为 IE 8 和 IE 9 开发应用程序，本书介绍了非常广泛的相关主题，但仍然不可能提供读者要找寻的全部答案。如果您在开发项目时遇到问题、注意到信息缺失，或者发现本书存在错误，建议您使用以下资源：

- Microsoft Developer Network (http://msdn.microsoft.com)：MSDN 是一个庞大的联机帮助文件，很多开发人员在为 Windows 操作系统开发应用程序时都会使用它。IE 拥有相当多的联机文档、文章和视频，尤其是在发布 IE 9 之后，更是如此。
- Code Project (www.thecodeproject.com)：对那些积极主动的 IE 扩展与应用程序开发人员来说，Code Project 是一个非常熟悉的资源。这里有大量的教程、开源示例和完整的项目，可以指导用户用各种语言来为浏览器开发最常见的扩展。

Microsoft CodePlex (www.codeplex.com)：CodePlex 是微软的开源项目站点。它为开发人员提供了存储、版本控制、升级和通信资源，用于开源开发项目。如果您正在寻找一个地方来张贴自己的 IE 项目，这里是一个非常不错的选择。

目　录

第 1 章

Internet Explorer 体系结构

Internet Explorer (IE)不只是一个 Web 浏览器，它还是一个非常广阔的平台，为 Windows 提供了一些必要的组件，用于将 Web 服务和和桌面应用程序集成在一起。它的复杂体系结构和扩展性，以及大量依赖它的应用程序，都反映了这一点。

本章将会从整体上概述 IE 的内部与外部组成，介绍浏览器及其库的体系结构，并为后面详细讨论主要功能区以及使用公开界面进行开发等奠定信息基础。

1.1 应用程序体系结构和相关项

IE 由一个浏览器应用程序和一系列库组成，这些库通过基于 COM 的体系结构联系在一起。这些二进制文件只能供 Windows 平台使用，从 IE 8 开始，能够在所支持系统的 x86、x64 和 IA-64 体系结构上使用。IE 8 可供 Windows XP SP2 及更高版本和 Windows Server 2003 及更高版本使用。

IE 浏览器是可执行文件、库及资源的一个松散集合，它们通过大量用于控制联网、文档托管、扩展性和标记处理的库函数，提供了一个用户界面(UI)和安全基础结构。例如，Trident 库(mshtml.dll)控制网页的分析、布局、呈现和显示。URL Moniker 库(urlmon.dll)封装 Windows 联网 API，为 IE 提供基础通信、安全性和下载基础结构。外壳文档查看(shdocvw.dll)提供了 WebBrowser 控件，它是一个得到广泛应用的库，将 IE 功能与独立应用程序集成在一起。

IE 依赖于由 Windows 和其他微软产品提供的大量界面和 API。Windows 相关项包括：使用 WinINET 进行缓存与 cookie 处理、通过 Windows RSS 平台实现源的组织与管理，以及通过“强制完整性控制(MIC)”和“凭据用户界面”来提供账户完整性保护。除了 Windows API，IE 还使用其他微软库，例如脚本引擎(JScript 和 VBScript)。

在 Windows Vista 及更高版本中，IE 实现了一组特殊的安全性 API，这些 API 针对权限与数据访问，在进程之间进行了明确隔离。诸如“保护模式”和“松耦合 Internet Explorer”等 IE 功能实现了上述基础结构，提高了浏览器的整体安全性、可靠性和效能。

IE 的一般体系结构(如图 1-1 所示)由一些可执行文件和 DLL 组成：

框架/代理进程(iexplore.exe，ieframe.dll)：这些进程用于控制 IE 的用户界面(浏览器“框架”)，控制对象通信和管理会话。

选项卡进程(iexplore.exe)：IE 的选项卡管理器和容器，用于显示网页和扩展。这一进

程受 IE 框架/代理进程的控制。

外壳文档视图/ShDocVw(shdocvw.dll)：MSHTML 和其他 OLE 活动文档(文档对象)的“活动文档容器”。这个库还公开了 WebBrowser 控件。

Trident/MSHTML(mshtml.dll)：一个代表 IE 布局、呈现和编辑引擎的“OLE 活动文档”对象。IE 就是用它来显示网页。

URLMon(urlmon.dll)：URL Moniker 库；用于封装 Windows 联网 API，并为 IE 提供基础安全性和下载管理。

WinINET(wininet.dll)：负责 Web 协议通信、响应缓存和 cookie 的 Windows 库。

源存储(msfeeds.dll)：Windows RSS 平台 API；由 IE 的 RSS 和 ATOM 源阅读器使用，以通过 Windows“通用源列表”打开、显示和管理源。

高完整性代理(ieinstal.exe)，ActiveX Installer Service (axinstsv.exe)：这些应用程序用来执行“高度完整性”操作(例如安装 ActiveX 控件)。

Internet 设置控制面板(inetcpl.cpl)：用于进行 IE 设置与配置的 Windows 控制面板界面。

HTML 应用程序宿主(mshta.exe)：WebBrowser 控件的一种实现，它以最小化的用户界面来运行受信任的 UI 和脚本。

JScript 和 VBScript(jscript.dll，vbscript.dll)：分别用于 JavaScript 和 VBScript 的主脚本引擎。

这个列表并没有包含 IE 的全部相关项和库，而只是列出了最重要的组件。在下面各章节中，将会更深入地研究 IE、其相关项以及 Windows 系统之间的交互。

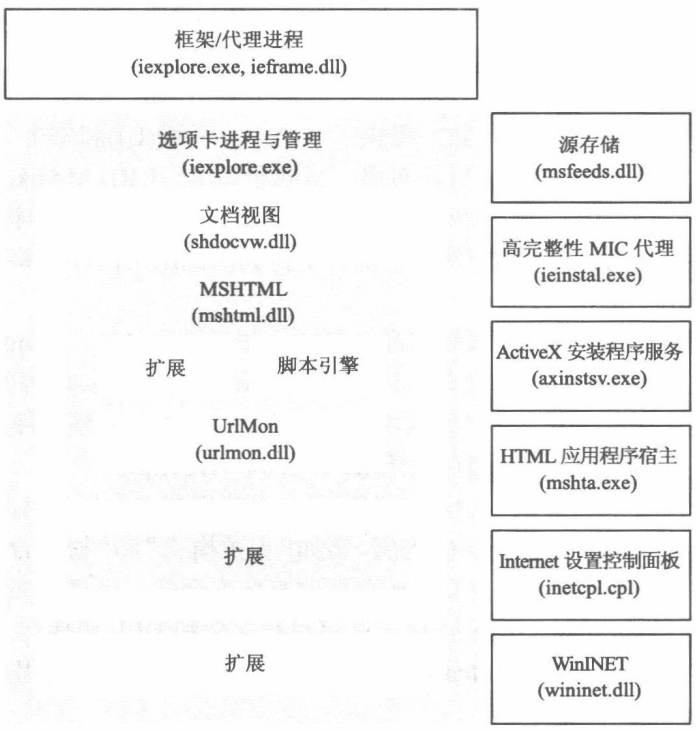

图 1-1　IE 的一般体系结构与应用程序

1.1.1　命令行参数

IE 可执行文件既可以通过命令行来运行，也可以提供自定义参数，以系统调用的方式运行。通过 IE 的命令行选项，可以对一个新进程进行基本配置；IE 的设置和功能控制将在后文讨论，利用它们可以精细调整浏览器的配置。

下面是 IE 提供官方支持的命令行参数：

```
iexplore.exe [-embedding] [-extoff] [-framemerging] [-k] [-noframemerging]
[-private][<URL>]
```

- -embedding：为 OLE 嵌入生成一个没有用户界面的 IE。
- -extoff：以“无加载项”模式运行 IE；为此 IE 实例关闭扩展。
- -framemerging：允许 IE 偶尔将新的框架进程合并到已经存在的进程中(但每个进程的窗口仍然是独立的)。
- -k：在 kiosk 模式、全屏、精简用户界面框架中运行 IE。
- -noframemerging：禁止 IE 将新进程合并到已有进程中。
- -private：以 InPrivate (私有浏览)模式运行 IE。
- <URL>：用于起始导航的目的 URL。

1.1.2　处理器支持

IE 8 提供了 x86 (32 位)和 x64 (64 位)两种安装包；64 位安装包中包含了每个 IE 二进制文件的 32 位和 64 位两种副本。在安装 Windows 操作系统时会默认安装 IE，所安装的 IE 包与 Windows 安装的体系结构相匹配；仅支持 32 位的安装包不能安装在 64 位平台上。截至本书英文版出版时，在该系统的默认浏览器中不能设置 64 位 IE，下文将解释其原因。

除了安装与设置限制之外，体系结构方面的限制也不允许在 64 位 IE 中加载 32 位扩展。也就是说，那些编译为 32 位库的工具栏、浏览器帮助程序对象和 ActiveX 控件，都不能放在 64 位容器中。例如，由于 Adobe 目前仅发布了 Adobe Flash 的 32 位版本，所以现在还不能在 64 位 IE 中加载它。

注意：

尽管 64 位 IE 相对于 32 位版本有一些优势(例如，默认情况下支持 DEP/NX 内存保护，理论上通过在本地执行 64 位版本而提高了性能)，但由于缺乏供应商(包括微软在内)提供的 ActiveX 控件和其他扩展，所以这一配置在通用浏览中是不可行的。不过，对微软来说，提供 64 位 IE 是很重要的，因为 64 位应用程序需要依赖于 64 位版本的 IE 库。

1.1.3　保护模式(低权限 IE)

Windows Vista 引入了 MIC 的概念，它使用完整性级别(IL)，通过信任、权限级别和用户账户控制来区分文件系统对象、注册表位置和 API，向用户发送提升请求(elevation request)。这种体系结构有助于防止不受信任的应用程序恶意访问系统和用户文件。

Windows Vista 和更高版本的完整性级别主要分为 4 个主要类别：

- 系统：核心操作系统权限(NTAUTHORITY)；系统组件、文件和数据
- 高：计算机级别访问权限(管理员)；程序文件和本地计算机注册表配置单元
- 中：用户级别访问权限(用户)；用户文件和设置、当前用户注册表配置单元
- 低：不受信任的内容、临时文件和数据

Windows 为通信处理和数据访问设置了一些基本规则。首先，进程只能向下发送命令，而不能向上发送；例如，以“低”级别运行的应用程序不能直接运行一个需要中级访问权限的 API，也不能访问需要中级访问权限的文件。其次，不同级别的进程只能通过该群组中的最低权限完整性级别进行通信；例如，如果一个中级进程和一个低级进程需要进行对话，它们只能通过一个具有低完整性级别的通道来实现，例如通过一个低完整性命名管道。最后，正在运行的进程不能在没有用户许可的情况下启动具有更高级别的新进程；例如，一个以中级权限运行的应用程序需要启动一个高级别的应用程序，用户将会看到一个 UAC 提示，以允许或拒绝该请求。对这个数据流，显然还有很多微妙之处和规则，但其基本前提很清晰：应用程序都获得一个许可级别，它们必须在此级别范围内操作，必要时，这些应用程序必须申请更高的访问权限。

保护模式是 IE 的一项功能，用于在 Windows 的完整性级别中分隔 IE 组件。IE 会触及操作系统的很多不同部分；例如，为实现缓存和 cookie 需要访问临时 Internet 文件，为实现用户预设置需要访问用户文件夹和注册表项，为了实现持久数据及计算机范围内 ActiveX 控件，需要访问计算机级别的文件和注册表项。IE 开发团队将这一非常广泛的访问权限与 Windows 的新 MIC 体系结构进行对比，最后得出结论：大量恶意攻击都可以通过这些控件得到缓解。因此，IE 现在分解为独立的进程、线程和通信控制器，使整个应用程序能够符合 Windows 在体系结构上的这一新的隔离方式。

保护模式用到了 Windows 体系结构的两个关键组件：MIC 和用户界面特权隔离(UIPI)。MIC 在前面已经提到，限制低级进程对高级位置和 API 的访问。保护模式依靠 MIC 来保护用户配置文件、注册表和 API(例如 OpenProcess()、OpenThread()和 CreateRemoteThread())，使其免受非授权访问。UIPI 是一种强制机制，它阻止向高级进程发送特定的 windows 事件消息。保护模式依靠 UIPI 来防止低级进程向更高级权限的进程发送潜在的恶意消息(也就是所谓的“粉碎攻击(shatter attack)”)。

IE 采用一种符合 MIC 体系结构的方式来分隔其进程和功能(如图 1-2 所示)。保护模式的网页被加载到以低完整性级别实例化的 iexplore.exe 进程中。默认情况下，在这一进程中工作的页面和扩展可以访问标有低完整性级别的临时 Internet 文件、使用标有低完整性级别的 API 和消息，并调用一组由高完整性级别 IE“代理”进程提供的安全 API。

一般来说，不受信任的网页内容非常适于采用低完整性级别，但这些限制也阻碍了在这种页面与其父框架之间进行非常基本的通信。例如，一个页面可能需要将其标题发送给父框架，以便在 IE 标题栏中显示，或者，一个页面可能需要启动一个 ActiveX 控件的安装。IE 框架进程允许低完整性级别通过 UIPI 执行高级别任务；较低完整性级别的页面可以要求代理框架进程为它们执行那些不允许自己执行的任务。

注意：

在 IE 7 中，中级完整性级别的代理是在 ieuser.exe 进程中实现的。而在 IE 8 中，ieuser.exe 中的功能被重构回 iexplore.exe 中，作为松耦合 Internet Explorer 实现的一部分。

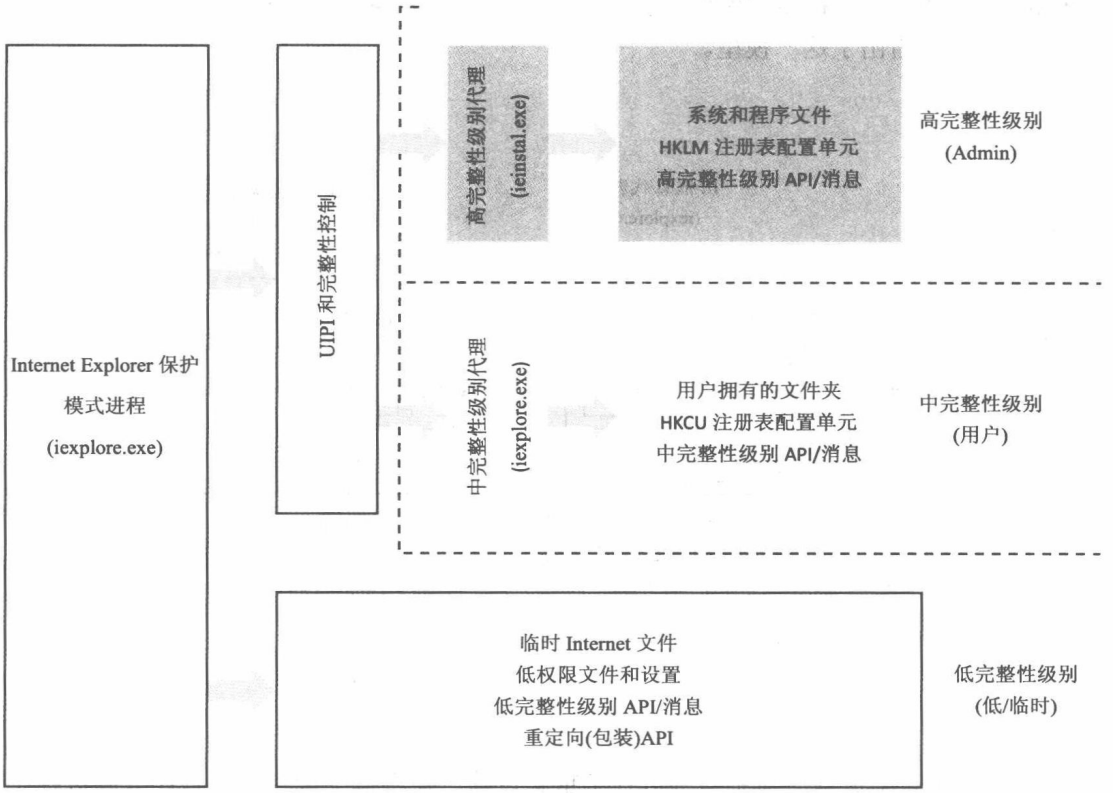

图 1-2　保护模式体系结构框图

在一个网页内容中运行的 ActiveX 控件、行为和其他扩展(也称为“内容扩展”)需要以其父进程的完整性级别运行。另外，在框架中可以看到的扩展(例如工具栏和菜单项、浏览器栏和工具栏)也必须符合这些新的策略。在刚引入 IE 7 时，这一变化导致了一个问题——大量加载项所依赖的 API 不能供那些以低完整性级别运行的进程使用。为了降低兼容性影响，IE 7 和 IE 8 提供了读/写虚拟化和包装 API。这些改变并没有解决所有兼容性问题，其中一些只能通过创建代理应用程序来缓解。在本章最后几章中将讨论这些 API 以及如何创建代理应用程序。

这一功能是受安全区域设置(将在本章后面讨论)控制的。在 IE 7 中，保护模式可以在“受限”、Internet 和 Intranet 安全区域中的所有页面上运行，而在 IE 8 中，它只能在前两者中运行。在未使用保护模式时，IE 进程的权限级别与当前用户账户的权限级别相同(在 Windows XP 中总是如此)。

并非对于所有页面或者所有 Windows 版本都使用了保护模式。在 Windows XP 和 Windows 2003 中，由于这些平台上没有 MIC 功能，所以也就没有“保护模式”功能。对于 WebBrowser 控件或 MSHTML 的主机，这一功能也是不可用的。

1.1.4　松耦合 Internet Explorer

松耦合 Internet Explorer(LCIE)是在 IE 8 中引入的，它利用进程分离来提高浏览器的可