若干重要的 Windows 参考资料

毛德操

要让 Linux 内核支持 Windows 应用程序和设备驱动，我们当然得要了解并理解 Windows 的各种机制和机理。本文的目的是为大家介绍和推荐一些关于 Windows 的参考资料。当然，对 Linux 的了解和理解更是必不可少，但是笔者以为既然是行走于我们这个地界的人，对 Linux 想必自有一定的基础，所以 Linux 方面的参考资料这里就不讲了。

说到 Windows 的技术资料，微软本身的各种 SDK、DDK、以及 MSDN 网站上的资料当然是重要的，但是信息量太大。在笔者看来，微软的资料数量之大正是由于不公开源代码。一件东西，放在透明的玻璃瓶里，自然就不需要作太多的描述；而若封装在一个黑盒子中，描述起来可就费劲了。微软既不肯公开其源码，却又想要别人在此基础上开发各种第三方软件，自然就得对其各种产品作黑盒子描述，“信息爆炸”就不可避免了。许多人见了微软的资料就烦，是因为这些资料只告诉你“其然”而不告诉你“其所以然”。也有许多人很喜欢微软的资料，是因为这些资料就像使用手册，所以“一抓就灵”。也难怪市面上有那么多关于 Windows 的各种“宝典”。读微软的资料可以使你成为“很好的”工程师，却不会使你成为科学家。

不过，幸而还有一些书，在讲述其然的同时还在讲述其所以然。有趣的是，其中特别重要的几本正是由微软出版社组织和出版的。可见微软自己也知道，光作黑盒子描述，光让人家知其然而不知其所以然，是不够的，那样很难成长起高质量的 Windows 软件开发人员，反过来对微软也不利。这跟奴隶主有时候也意识到该让奴隶们吃的壮实一些，是同一个道理。

而对于我们，这些书的重要性就不言而喻了。

Windows 参考书的首选当推 Mark Russinovich 和 David Solomon 的“Microsoft Windows Internals”第 4 版，微软出版社 2005 年版。我们只要简单回顾一下这本书的历史，读者就可体会到它的重要性。这本书的第一版由 Helen Custer 编写，书名“Inside Windows NT”。第二版(1998 年)改由 David Solomon 编写，由 WinNT 开发团队的主任 Lou Perazzoli 作序。第三版(2000 年)的书名改成“Inside Windows 2000”，由 David Solomon 和 Mark Russinovich 共同编写。到了第四版，书名又改成“Microsoft Windows Internals”，由 Mark Russinovich 和 David Solomon 共同编写。尤其引人注目的是，第四版上有 David Cutler 写的前言，题为“Historical Perspective”，文中回顾了 WinNT 的由来。这位 David Cutler 可不是等闲之辈，他是 WinNT 之父。就是他，当年把 VMS 的技术和(部分)人马从 DEC 带到了微软。有个笑话很形象地说出了 WinNT 和 VMS 之间的渊源关系：把“VMS”这三个字母的 ASCII 代码每个都加 1，就成了“WNT”。而 David Solomon 是 David Cutler 在 DEC 就相识的老伙伴。正是 David Cutler 特许 David Solomon 可以自由翻看 WinNT 的源代码。这种“看”，跟把人请去住在旅馆里十天半个月、每天去微软资料室看上几个钟头的那种“双规”下的“看”，

当然有着天壤之别。所以，这本书应该说是一本权威著作，书中所讲应该认为是有源代码根据的。再说，这本书也确实让人知其然并且知其所以然。当然，要是有源代码就更好了，但是要知道那是微软，能有如此这般就很不错了。在兼容内核的开发过程中，这本书无疑将在总体上起很大的指导作用。

第二本书是 Walter Oney 的“Programming the Microsoft Windows Driver Model”第 2 版，微软出版社 2003 年版。这本书对微软的 WDM 设备驱动模型(即框架)作了深入的介绍。微软要求从 Win2k 开始的设备驱动模块都符合 WDM 的要求。与传统的 WinNT 设备驱动相比，WDM 要求设备驱动模块都支持 PnP(即插即用)、电源管理(不用时可转入省电模式)、以及 WMI(Windows Management Instrumentation，意为 Windows 管理手段，是微软版的 WBEM 实现)。所以，这本书所介绍的是新的 Window 设备驱动框架的设计与实现，附带着也介绍了设备驱动界面上的一些重要的函数。显然，这本书对于兼容内核中设备驱动框架和设备驱动界面的实现有着重要的指导意义。读了这本书，再回过去看 Windows DDK 中一些样本实例的源代码，就更容易理解，理解也可以更深了。

不过，现在实际上在使用的.sys 模块还有不少只是传统的 WinNT 设备驱动。WinNT 的设备驱动框架可以说是 WDM 的一个子集，比 WDM 要简单一些。对于 WinNT 设备驱动，Art Baker 的“The Windows NT Device Driver Book”是一本很好的参考书。这本书是由 Prentice Hall 在 1996 年出版的。虽然年代已经久远，书的内容却并不显得太陈旧，可以作为 WDM 那本书的补充，参照阅读。

第四本书是 Jeffrey Richter 的“Advanced Windows”第 3 版，微软出版社 1997 年版。这本书就不仅仅是讲内核了。它让读者对 Windows 操作系统有个整体上的理解。例如，在另一篇文章中笔者曾提到，Windows 在创建子进程时对于已打开文件的遗传与 Unix/Linux 在方式上有很大的不同，这本书对此就有很详细的叙述。而这一点正可以说明，不同内核间的有些差别是很难在内核外面得到补偿的。

第五本书是 Gary Nebbett 的“Windows NT/2000 Native API Reference”，MTP 出版社。这里所说的“Native API”，实际上就是系统调用。显然，这是一本关于 WinNT 系统调用的参考手册。既然微软把系统调用界面藏在黑盒子里面，或者说藏在 Win32 API 后面，从来都不公开，那么这本参考手册的价值也就不言而喻了。看一下这本书，就可以知道实现 Windows 系统调用界面的工作量该有多大。

作为对这本书的补充，Parasad Dabak 等人的“Undocumented Windows NT”，M&T Books，1999 年出版，对于 WinNT 系统调用的实现也是一本有用的参考书。与前面几本由微软出版的参考书不同的是，这两本书的材料主要是通过逆向工程得来的。有源代码作为根基的著作固然比较权威，根据实验取得的资料也值得重视。

还有一本 Sven Schreiber 的“Undocumented Windows 2000 Secrets”，Addison-Wesley，2001 年出版，也是一本好书，甚至更好。这本书一边是基于逆向工程介绍 Windows 内核各方面的内容，也包括设备驱动；另一边还教给读者一些逆向工程的方法，所以对程序的调试

很有好处。特别值得一提的是，这本书的附录中实际上还列出了 Win2k 系统调用的函数跳转表、即函数名与系统调用号的对照，书中还讲述了这个对照表是如何得来的。这可是个宝贵的信息。因为 Native API 一书中虽然详细介绍了各个具体系统调用的使用方法，却并未提供它们的系统调用号。而若缺了这个信息，我们在实现 Windows 系统调用界面的函数跳转表时就得多费许多周折。

最后，Rajeev Nagar 的“Windows NT File System Internals”，O’Reilly，1997，虽然主题是“文件系统内幕”，但是实际上对内核的各个方面都有一些介绍，也有一定的参考价值。

这八本书是笔者所知最好的 Windows 参考书。当然，并不是说读者必须读了这八本书的全部才能从事兼容内核的开发，更不是说读了这八本书就一定可以把兼容内核开发好。

参考书目

Mark Russinovich，David Solomon，“Microsoft Windows Internals”，4e，Microsoft Press，2005

Walter Oney，“Programming the Microsoft Windows Driver Model”，2e， Microsoft Press，2003

Art Baker，“The Windows NT Device Driver Book”，Prentice Hall，1996

Jeffrey Richter，“Advanced Windows”，3e，Microsoft Press，1997

Gary Nebbett，“Windows NT/2000 Native API Reference”，MTP, 2000

Parasad Dabak, “Undocumented Windows NT”，M&T Books, 1999

Sven Schreiber，“Undocumented Windows 2000 Secrets”，Addison-Wesley，2001

Rajeev Nagar，“Windows NT File System Internals”，O’Reilly，1997