《x86汇编语言》

图书基本信息

书名：《x86汇编语言》

13位ISBN编号：9787121187995

10位ISBN编号：712118799X

出版时间：2013-1

出版社：电子工业出版社

作者：李忠,王晓波,余洁

页数：375

《x86汇编语言》

内容概要

《x86汇编语言:从实模式到保护模式》采用开源的NASM汇编语言编译器和VirtualBox虚拟机软件，以个人计算机广泛采用的Intel处理器为基础，详细讲解了Intel处理器的指令系统和工作模式，以大量的代码演示了16／32／64位软件的开发方法，介绍了处理器的16位实模式和32位保护模式，以及基本的指令系统。

《x86汇编语言:从实模式到保护模式》是一本有趣的书，它没有把篇幅花在计算一些枯燥的数学题上。相反，它教你如何直接控制硬件，在不借助于BIOS、DOS、Windows、Linux或者任何其他软件支持的情况下来显示字符、读取硬盘数据、控制其他硬件等。《x86汇编语言:从实模式到保护模式》可作为大专院校相关专业学生和计算机编程爱好者的教程。

《x86汇编语言》

书籍目录

《x86汇编语言》

章节摘录

版权页： 插图： 第13章 程序的动态加载和执行 像我一样，很多人在了解了保护模式的基本工作原理之后，会产生一个疑问。那就是，所有的段在使用之前，都必须以描述符的形式在描述符表中进行定义，那么，像操作系统这样的软件，又怎么能够加载和执行其他各种用户程序呢？毕竟，你并不知道这些程序都定义了哪些段，每个段是什么类型，有多长。 未必所有人都会产生这样的疑惑，但我确实算一个，可能我还不够聪明。事实上，这仅仅是一层窗户纸，一旦捅破了，才发现原来竟是那么简单。从某种意义上来说，保护模式的工作机制对用户程序的加载和执行非但没有增加困难，反而带来了很大的便利。 一套能够充分说明问题的例子需要很大的代码量，也许把本书的汉字都去掉，全部换成代码也不够。不过，只要能说明问题，也不一定非得完善周全、面面俱到。因此，本章中用于加载和处理用户程序的做法，不一定，甚至根本就不是操作系统采用的方法。这一点，务必明了。 计算机硬件之上是软件。软件分两个层次，一是操作系统，二是应用（用户）程序。通常，用户程序只关心问题的解，就是采用各种算法来解决实际问题。至于软件是怎么加载到内存的，怎么定位的，不是它所操心的事。但是，它有义务提供一些必要的信息，来帮助操作系统将自己加载到内存中。 相反，操作系统则必须考虑采用什么方法来加载用户程序，并在适当的时候将处理器的执行流转移到用户代码中去。同时，为了减轻用户程序的工作量，操作系统还应当管理硬件，并提供大量的例程供用户程序使用。比如，显示一个字符串，就不要让用户自己来写代码了，直接调用操作系统的代码即可。但操作系统和用户程序应当协商一种机制，让用户程序能够在使用这些例程时，不必考虑和关心它们的位置。 本章提供了一个小小的“ 操作系统 ”，因为当不起这么大的名称，所以叫“ 内核 ”或者“ 核心 ”。即使是这样，它依然当不起，因为它实在是太简单了。不过，也没有办法，就这么凑合着叫吧。 内核不能放到主引导扇区里，毕竟它都很大。所以，计算机首先从主引导程序开始执行，主引导程序负责加载内核，并转交控制权。然后，内核负责加载用户程序，并提供各种例程给用户程序调用。提供给用户程序调用的例程也叫应用程序接口（Application Programming Interface，API），本章用简单的方法来允许用户程序使用API工作。 本章学习目标： 1.了解保护模式是为操作系统提供的技术，并没有给普通应用程序的编程带来负担（这从本章的程序实例中就可以看出来）。 2.学习操作系统在保护模式下加载和重定位应用程序的一般原理，学习简单的内存动态分配，了解应用程序接口API的简单原理，学习字符串的比较算法。 3.学习若干x86处理器的新指令，包括bswap、cpuid、cmovcc、sgdt、movzx、movsx、cmpsb、cmpsw、cmpsd和xlat等。

《x86汇编语言》

编辑推荐

《x86汇编语言:从实模式到保护模式》主要讲述INTEL x86处理器的16位实模式、32位保护模式，至于虚拟8086模式，则是为了兼容传统的8086程序，现在看来已经完全过时，不再进行讲述。《x86汇编语言:从实模式到保护模式》的特色之一是提供了大量典型的源代码，这些代码以及相配套的工具程序可以到书中指定的网站，或者电子工业出版社华信教育资源网搜索下载。

《x86汇编语言》

精彩短评

1、开发操作系统的第一步，学习汇编的必备
2、我不知道正版书籍什么样子，但是这本书发过来，纸张很薄，而且页面发黄，像是旧书。页角都褶皱了……快递速度还好。
3、非常好的一本汇编方面的书，有别于其他一开始就上来一堆指令介绍的书，本书以一种演绎的方式讲述了汇编到计算机体系结构的方面的知识，读来知其然也只其所以然。另外，攒下作者的叙事条例和不错的文字功底
4、个人看过的x86汇编讲解最系统，最细致的一本书。
5、挺实用的，书真的不错，还会来买
6、偶然的机会在书店读了这本书，以前读过王爽写的汇编语言，看到最后发现仅仅讲了实模式的汇编语言，而没有保护模式的汇编语言，觉得很遗憾，而其他的保护模式的书，说实话，我也看过，但是实在是读不下去。而这本书的语言确实比较不错，读起来并不觉得枯燥，更重要的是。实验配置的很好，如果你想写一个小型的操作系统内核，这本书，再适合不过了，因为全书的实验就是在无操作系统的环境下讲解的，从引到扇区开始讲解，最后到如何跳转到保护模式，并且作者自己编写了一个不叫内核的内核，用来加载用户的程序。
我个人觉得，在不参考配套源码的情况下，如果看着书的讲解，自行编写程序，并运行和调试程序，最后再对照配套源码，收获更大，我是在linux下，做的实验。而没有使用作者提供的在windows下的工具。觉得收获很大。
另外书也是有错误的，很明显有很多错别字。不过并不影响阅读，
还要再说一下，同样是一本武林秘籍，在不同的人手中，发挥的作用和效力也是不同的，既然买下了这本书，希望能坚持看完。
全力推荐。
7、书很好，讲解很清楚
8、好，这本很好，这本真的很好。
9、很好的计算机资料，能系统的学习汇编
10、很不错的书，是我的入门书呀
11、内容简单易懂，较实用，非常不错。
12、还行吧，为什么要5个字
13、书很好，装订不错，内容也很好，值得一读。
14、非常系统这本书
15、X86实模式到保护模式是我看过所有书里讲的最明白的。力荐。
16、最近翻了翻这本书，这是一本通俗的Assembly的书，看得出作者对自己所写的已经吃的很透，而且下了不少功夫。本来low level的编程就没那么神秘，只是不合格的教育让这些神秘化了。但是作为书籍，我觉得可以在方便阅读上做点更多的考虑。书中可以一边列源码，一边讲解，利于在厕所里或者在床上看。另外，有些地方写的有些罗嗦和重复，可以更加简洁。希望下一版改进。
17、学完后可以看X86X64体系探索与编程（也是用NASM）和自己动手写操作系统通过实践学习操作系统
18、买这本书是为了在看“一个操作系统的实现”之前有个铺垫。本书对实模式和保护模式的讲解非常详细明白，并且我也看懂了，也写出代码折腾了。但是之后有关操作系统的部分就只适合了解，不是那么值得实践了。主要原因在于书中的例子都是作者自己的作品，我觉得如果涉及到实践，不如去读Linux的源代码。
19、面向的是汇编入门者，但是后几章真的是很不错，读完之后会对实模式和保护模式、系统的基本引导过程、中断的过程、程序的执行过程有非常清楚的了解。
20、很棒的一本书之前读过作者的《穿越计算机的迷雾》一书
21、这本书不错，采用任务推动模式，讲的也挺好，不过还是需要先看点儿基础的知识。另外书里有一些错误，看的时候不知道能坑死初学者，建议买了之后上网查查订正信息。
22、前面部分讲得不错
23、我发现这书上提的有光盘，光盘呢？

24、之前看过被奉为经典的王爽老师的汇编教程，那真的是简明易学，但是总觉得和实际运用不太沾边，毕竟8086的时代还是太遥远了，作为奠基性的学习还是有必要的；罗云彬的Win32汇编教程同样也是经典，但那本书主要立足于Win32平台下的API编程，对于保护模式的机制并没有做过多的讲解（开头提了一下）。这本书正好弥补了两者之间的断层，另外，这本书使用NASM编译器，让我们这种熟悉了MASM的人开始有些不适应，不过慢慢习惯就好了，毕竟只是编译器而已。
25、还行，只是过于简单了点，拿来做入门还是可以的。保护模式写得还行。
26、正版，还很便宜，支持网购
27、还行，但是还有不少地方需要再细化的。希望作者在第二版中补充
28、非常好，值得购买，此书填补国内空白。作者在书中的语言平易近人。只要认真阅读本书，肯定能学到东西。
29、比本科的汇编教材要好很多，非常实用 。
30、第一次认真反复看的书，受益不少。感谢作者！不知道是否有勘误表，阅读中发现了一些瑕疵，想对照一下。
31、写的不同于一般的教科书，适合自学的人
32、快递给力，当当不给力，给了本95成新的书，不是全新的。里面的内容还是不错的。
33、内容很好，很好，很好，很好。
34、保护模式将的不错。学不会保护模式的可以买了，实模式感觉跟王爽老师的没法比。
35、看了前半本，和《穿越计算机的迷雾》相比，可是差的太远了；递进的逻辑性没有了。也不成体系，没有太大参考价值。
36、买了学习使用的，送货上门很方便的！很合适@
37、这是我见过的写汇编写得最深入的一本，的确写了很多不为人知的细节，一个字，赞
38、看了作者放出的样章，最大的感觉是废话太多。作为有兴趣（或需求）来学习汇编语言的读者，应该都已经有相当程度的计算机基础知识。鉴于此，作者应该尽量减少一些无关（或过于详细）的背景介绍。由于看了很久都没有开始真正的”硬货“（浏览了后面的章节，貌似”硬货“也是夹杂在一堆东拉西扯之中），我不得不失望的先放下它。转而拿起nasm手册姑且读之。。。... 阅读更多
39、在看感觉还行，先了解一下
40、书的材质我很满意。 但是不小心地址填错一个字，竟然没人联系我、 直到我自己发现
41、要开始干操作系统的同学建议先用这本书来补一补汇编。
42、通俗易懂吧，引领我对系统了解的入门神器
43、想写x86机器上的操作系统必看！比于渊的书强多了！！
44、破书一本，这里讲点那里讲点，会了看了也没用，不会看了照样不会，还是去看三卷本把，买后悔了
45、内容详实，适合初学者
46、这本书从基础讲起，很详细，值得一看
47、个人觉得弥补了 罗云彬32位 和 王爽16位的的中间部分~~~还是不错的~~
48、书的内容没得说，写的很用心，不像国内的课本那样语言生硬。不过这纸实在对不起这价钱，真是薄的半透明了
49、书的内容还行,适合初学汇编的朋友,但是印刷质量实在不怎么样, 纸很薄。
50、不错，有启发，或者说作者都告诉你了。
51、内容经典不错，值得买
52、不错的好书，需要耐心看完。
53、简单易懂!
54、看完了，还可以，但其实没有耐心看完快一千行用汇编写的四不像内核，把保护模式讲清楚就行了，想了解OS就去看专门讲OS的书。
55、对于作者,曾在群里和他交谈过.他确实厉害,就是比较贪钱.哎.
56、看王爽的书后，想了解下保护模式，实模式的。
电子版网上有下不过不全，代码和工具相关的网上也能找到
57、内容经过作者验证，逐步分析，有实践经验的人写的，不过13章-2的程序编译通不过，后面的程序有点大，看的头疼

58、很不错的书，学完了王爽的实模式汇编后再来看本书更是受益匪浅
59、今天刚收到书，内容不错，是我想看的。但是书的纸质太差，都能看到下一页的内容，从纸质来说，此书定价偏高。
60、作者苦口婆心，兼顾到初学者和有一定基础的同学需要，循序渐进，从最基础的2进制开始逐步升入，讲得透彻。国外同类书籍虽然都讲的细致、透彻，但篇幅实在可怕。这本篇幅虽然不大，却涵盖了汇编的所有基础性内容，其深度不亚于一部美国的大部头，让我想到了中国传统智慧四两拨千斤的巧劲。相比较而言，王爽的书还是多多少少有些国内教科书的味道，有点“冷冰冰”，对读者的考虑不是很够。国... 阅读更多
61、书很好,就是书皮有些脏,擦擦就好。
62、很少有讲nasm的书 这本不错
63、非常系统能的学习汇编，实模式及保护模式讲解的非常清楚，正如作者所言，非常舍得大家一读。
64、2012-2014，通过这本书学习了汇编，以及驱动编程。
65、目前读过国人自己写的汇编书籍中最好的一本。王爽的汇编固然好，但是内容还是太老了。这本从实模式讲到保护模式，基本上x86下面写一个简易内核需要涉及到的汇编知识都有。
66、汇编本来就和操作系统不可分的。这本书还原汇编的本质，在操作系统的基础上进行讲解。适合用来学习汇编
67、讲还很比较直观容易懂。
68、简单明了
69、对汇编学习来说，内容一般偏上吧。还没有到非常好
70、大部分书都是介绍8086的而且语法偏多。这本书就好很多，实用性比较强。汇编语言么，偏操作系统和硬件才好。
71、作者技术功底和语言功底都不错，看起来很舒服，说得也很清楚。

《x86汇编语言》

精彩书评

1、恳请创建者更改为《x86汇编语言：从实模式到保护模式》.不然就违背了作者本身意图。大家可以加我的QQ：1658843124 进行讨论，我们一起互相学习，互相交流，也会有作者的亲自指点。谢谢大家评论字数至于这么多吗？

《x86汇编语言》

章节试读

1、《x86汇编语言》的笔记-第10页

处理器由很多的引脚，通过它们来传送点信号,引脚是复用的,所以当你传送完电信号,可能后面也会传送来电信号,这时电信号的会送入一个称为 寄存器 的电路锁住(存储),以便下一个电信号进行传送
通过引脚传送到CPU内存的那条线叫做 内部总线 并不知道描述的对不对,仅此发表个人观点,望以后的我加以改正
这个引脚从作者提供的图样来看像一根一根的小刺似的 本人并没有看过
CPU 内部还有一个算数逻辑部件 用来数值运算的电路

关于一个加法运算的简易流程：
通过引脚传送电信号(加数) 通过 内部总线 传入 寄存器 RA 电路并锁住(存储)
接着 通过引脚传送电信号(被加数) 在通过 内部总线 传入寄存器 RB 电路并锁住(存储)
然后 通过 算数逻辑部件 将 RA 与 RB 相加 然后产生的结果送入 临时寄存器R3
然后可能这个结果送入CPU外部 或者 送给 另一个寄存器 或存储空间

虽然步骤说的很慢 对于CPU 来说处理这个流程时会相当迅速

还有一个控制器 作者并没有在图中画出
它呢 作者简述说到 负责给各个部件发送控制信号（我认为上面提到的 加法运算流程 会不会是由这个控制器来控制算数逻辑部件不然传送加数和被加数后 为什么会进行 加法
可能这个控制器改写了某个位吧 然后这个 算数逻辑控制部件检测到后就知道要计算了
我怀疑 RA RB 这两个寄存器是固定专门用来存入加数和被加数的然后逻辑部件进行运算的时候只许要将RA 和 RB 进行预算即可 而不用去过多的检测那个是被加数寄存器和加数寄存器 [个人观点,待以后的自己改正] ）也负责控制那个部件由权限使用 内部总线
感觉像个 交通警察 一样 协调交通的一样

作者说到 CPU 很繁忙, 寄存器里的数据只能暂时存储一会儿之后就会被新数据覆盖掉
个人疑问:假如一些重要的数据的传输 会存给寄存器吗？
之后又谈到了 寄存器 的存储空间相关的知识
1个字节(Byte)=8个位(Bit) 需要注意的是 有些人喜欢简写 那… 1b 代表什么呢？ 字节还是位 如果为了区分 我还是觉得这个样写比较好 B代表字节 b 代表位 便于区分 但看到这章节作者并没有提出
我给出一些 基本单位吧
1 (Byte)=8 (Bit)
1 (MB)=1024(Byte)
1 (GB)=1024(MB)
1 (TB)=1024(GB)

继续回到话题 早期的寄存器有 4位 8位 16 位 现在呢是 32位 64位之多
这意味着什么呢 寄存器 的位数越大是不是我们的存储的数据越来越多 就像 作者在前几节课中所讲到的一样 计算机 是以二进制数据的形式存储的,所以说你的寄存器 位数越大越能满足我们的存储需求也可以简化程序 比如以前的4位寄存器 在存储很大的数据的时候怎么办？一个寄存器不能存储 就要用别的方法或占用多个寄存器 现在呢 32位 64位的啪啪啪的向里存入数据 多方便存储容量大 就坚决的程序不必要的麻烦

这里呢又提到了字的概念 就是 2B(字节) 就等于 1个字 只需要记住既可
双字呢 也就是 4B(字节) 就等于 2个字 是一种规定吧,我们遵守既可

《x86汇编语言》

我认为这个章节里我认为重要的一点就是理解 最高有效位 和 最低有效位 和 高字 低字

高字 低字
二进制：1000 0000
编号：7654 3210
这是一个8位寄存器 也就是存储了八个位 注意这里还有编号 是从右向左的
开始的编号是从0 开始的 需要记住
可以看出 对于8位寄存器 0~3 是它的低字 4~7是他的高字
可以这样计算: 低字等于= 0 ~ 8(位位数)/2-1 高字等于= 8(位位数)/2 ~ 8(位位数)-1
16 进制呢 只需要将8 改成16 既可

最高有效位是: 编号7 的那个位数 最低有效位当前是:编号0 的那个位数（这是不变的）
具体的请看书的 12 页

2、《x86汇编语言》的笔记-第32页

这一章主要介绍实验环境。大学时候学过计算机原理和操作系统课程就体会到实验对于这些基础系统课程的重要性，在这一点上，作者做得非常好，不仅仅每一章都有实验相关内容，而且还自己写了一些软件来支持这些实验内容，更值得称赞的是还介绍了如何用bochs来做一些调试的工作，包括单步执行，观察CPU状态的，这一部分对于理解x86是非常有帮助的。反正单步执行时，观察到寄存器、内存等内容的变化是，还是觉得很有意思的。美中不足的是实验环境是基于windows的，由于我自己用mac，所以还是换了一点功夫摸索出在mac上如何创建实验环境，包括安装bochs，用dd替代作者写的FixVhdWr等等，等以后有时间可以再写写。
发现用带GUI的bochs调试更方便，下面是截图：

3、《x86汇编语言》的笔记-第10页

日本人在1971年受到Intel公司的启发 制作了第一个处理器 Intel 4004
CPU从内存里读取指令,并触发相应的操作,通常情况下是连续不断,循环反复的。
CPU是一台电子计算机的核心部件

《x86汇编语言》

版权说明