南開大學

汇编语言与逆向技术课程实验报告

实验二： dex2hex

学　　院　网络空间安全学院
专　　业　信息安全、法学双学位
学　　号　2212000
姓　　名　宋奕纬
班　　级　1061

一、实验目的

1、 熟悉汇编语言的数据传送、寻址和算术运算；

2、 熟悉汇编语言过程的定义和使用；

3、 熟悉十进制和十六进制的数制转换

二、实验原理

1、 实验环境：MASM32 编译环境、Windows 命令行窗口

2、 实验思路：分为两步——dex to dw 以及 dw to hex

（1） Dex to dw:将十进制数字符串转化为十六进制数

将输入的十进制字符串的每一个字符依次提出，减去 48（即字符’0’的 ASCII 码）即可转化为该字符对应的数值，将该数值与已存储数值乘 10 得到的结果相加进行存储，存入寄存器后，就可以自动转化为十六进制数，进行循环，即可将输入的十进制数字符串转化为十六进制数。

（2） Dw to hex：将十六进制数转化为十六进制数字符串

将十六进制数的倒数第 i 位向右移 4*（i-1）次，将其放到寄存器的最右位,然后再指向该位的数字值。当数字值小于等于 9 时，依次将数字值加上 48（30h）得到其对应的字符的 ASCII 码；当数字值大于 9 时，依次将数字值加上 87（57h）得到其对应的 A-F 的 ASCII 码。循环依次存储，但此时存储的是从低位向高位，为正确的字符串的反向字符串，故再进行反向存储的过程，将字符顺序反向，即可得到正确的十六进制数字符串。

三、实验过程

1、指定处理器、指令集，指定内存模式，引入头文件，链接静态库文件。

```
.386
.model flat,stdcall
option casemap :none
include \masm32\include\windows.inc
include \masm32\include\kernel32.inc
include \masm32\include\masm32.inc
```

```
includelib \masm32\lib\kernel32.lib
includelib \masm32\lib\masm32.lib
```

2、定义数据段，进行相关数据的定义、声名和初始化。

```
.data
decstr byte 20 DUP(0);定义一个字符数组，用于存储输入的十进制数的字符串
w byte "Please InPut Your Number:",0 ; 定义提示语
decnum DWORD 0 ;用于存储每一次转换后的结果
const10 DWORD 10;对常量进行定义（此处定义的是除数）
hexstr byte 9 DUP(0);定义一个字符数组，用于存储得到的十六进制数的字符串
```

3、Dec2dw 过程的书写

```
dec2dw PROC
    mov esi ,0                  ;清0
    mov ebx,0                   ;清0
L1:
    mov edx,0                   ;清0 ，用于存储当前字符对应的数字值
    mov bl,[decstr+esi]         ;从字符串中读取一个字符，并存在寄存器bl
    sub ebx,48                  ;ASCII码表示的字符转换为对应的十进制数值
                                ;字符'0'到'9'的ASCII码值分别是48到57。
                                ;将EBX寄存器中的值减去48，可以将字符'0'
                                 到'9'转为相应的数字0到9。
    mov eax,decnum              ;将decnum中存储的转换结果加载到eax中
    mul const10                 ;将eax寄存器存储的值*10，并把结果存储
    mov decnum,eax              ;将乘法运算后的结果存储回decnum中，更新
                                 转换后的结果
    add decnum,ebx              ;将ebx寄存器中接收数字对应的数字值加到
                                 decnum中
    inc esi                     ;将esi寄存器的值加1，指向下一个待转化的
                                 字符
    mov bl,[decstr+esi]         ;从字符串中读取下一个字符，并存在寄存器
bl
    cmp bl,0                    ;比较bl中的值和0的关系
    jnz L1                      ;若bl中存的值不为0，即还有未处理字符，则
                                 跳转至L1标签处，再次循环处理
    ret
dec2dw ENDP
```

4、Dw2hex 过程的书写（此处报错过程冲突，故修改过程名为 zhuanhua）

```
zhuanhua PROC
    mov esi, 0              ; 清0
```

```
    mov ecx, 8                ; 循环8次，每次处理4位二进制数
L2:
    mov eax, decnum           ; 将十进制数存储在eax中
    and eax, 0Fh              ; 取出eax中的低4位，即一个十六进制数位的值
    cmp eax,                  ; 判断是否大于9
    jbe LessTha               ; 若小于等于9，跳转到LessThan9标签处
    add eax, 7               ; 若大于9，将其转换为A~F的ASCII码值
LessThan9:
    add eax, 30h              ; 将数字值转换为ASCII码值
    mov [hexstr+esi], al      ; 存储转换后的十六进制字符
    shr decnum, 4             ; 将十进制数右移4位，相当于去掉一个十六进
                                制数位
    inc esi                   ; 指向下一个存储位置
    loop L2                   ; 循环处理8次，直到处理完所有十六进制数位

    ; 反转存储的十六进制字符
    mov esi, 0                    ; 清0
    mov edi, 7                    ; 指向最后一个字符
L3:
    mov al, [hexstr+esi]          ; 从低位开始取出字符
    mov dl, [hexstr+edi]          ; 从高位开始取出字符
    mov [hexstr+esi], dl          ; 将高位字符放到低位位置
    mov [hexstr+edi], al          ; 将低位字符放到高位位置
    inc esi                       ; 指向下一个低位字符
    dec edi                       ; 指向上一个高位字符
    cmp esi, edi                  ; 比较指针位置，如果相遇或交叉，则结束
                                    反转
    jge L4                        ; 跳转到L4标签处
    jmp L3                        ; 继续循环反转

L4:
    ret
zhuanhua ENDP
```

5、运行部分

```
    start:
        invoke StdOut, addr w         ; 输出提示信息
        invoke StdIn, addr decstr, 20 ; 获取用户输入的十进制数

        call dec2dw                   ; 将ASCII字符串转换成DWORD数据
        call zhuanhua                  ; 将DWORD数据转换成十六进制字符串

        invoke StdOut, addr hexstr    ; 输出十六进制字符串
```

```
    invoke ExitProcess, 0          ; 程序结束，退出
end start
```

6、进行汇编操作：使用 ml 将 dec2hex.asm 文件汇编到 dec2hex.obj 目标文件。

```
D:\>\masm32\bin\ml  /c  /coff C:\Users\宋奕纬\Desktop\dec2hex.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997.  All rights reserved.

 Assembling: C:\Users\宋奕纬\Desktop\dec2hex.asm

************
ASCII build
************
```

7、进行链接操作：使用 link 将目标文件 dec2hex.obj 链接成 dec2hex.exe 可执行文件。

```
D:\>\masm32\bin\link /SUBSYSTEM:CONSOLE D:\dec2hex.obj
Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.
```

8、测试运行

```
D:\>D:\dec2hex.exe
Please InPut Your Number:1000
000003E8
D:\>
```

输入了 1000 进行测试，输出其 16 进制数 3E8.

四、实验结论及心得体会