Assembly x86

Hugo Bessa - hrba
Paulo Serra Filho – ptvsf

Roteiro

- Assembly
- Assemblers
- Sections
- Registradores
- Registradores de Segmentos
- Principais Operações do NASM
- Funcões e Macros
- Interrupções
- Compilando um programa

Assembly

- Linguagem de baixo nível
- Traduzida por assemblers
- Baseada em mnemônicos
- Assembly x86 diferente do MIPS
    - Menos registradores
    - Muitas operações podem ser feitas com dados na momória
    - Maior abstração

Assemblers

- TurboASM - TASM
- MicrosoftASM – MASM
- NetwideASM - NASM
    - Gratuito
    - Unix
- Um assembler não compila o código de outro

Assemblers

- NASM: por que usar?
  - Sintaxe menos poluída
  - Mais abstrações
  - Opensource

```
;Programa 1
section .data
arq: db 'texto.txt',0
error: db 'impossivel criar arquivo',0Ah
tam :equ $-error ;$

section .bss
char: resb 1

section .text
global _start
_start:
;Seu código aqui
mov eax,1
mov ebx,0
int 80h
```

Sections

- `.data`
  - Dados inicializados
    - `db` ;Declara bytes
    - `equ` ;Resolve uma expressão e inicializa a variável com o resultado
    - `dw` ;Declara uma palavra que armazena um dado
  - Ex:

```
section .data
        message: db 'Hello world!'
        msglen: que 12
        buffersize: dw 1024
```

Sections

- `.bss`
  - Espaço reservado (variáveis)
    - `resb` ;Reserva uma quantidade de bytes
    - `resw` ;Reserva uma quantidade de palavras(2bytes)
    - `resq` ;Reserva um array de numeros reais
  - Ex:

```
section .bss
        name: resb 255
        bigNum: resw 1
        realarray: resq 10
```

Sections

- `.text`
  - Onde o código assembly fica
  - Ex:

```
section .text
        global _start
_start:
        POP EBX
        .
        .
        .
```

Registradores

- 32 bits
  - EAX
  - EBX
  - ECX
  - EDX
  - EBP
  - ESI
  - EDI
- 16 bits
  - AX
  - BX
  - CX
  - DX
  - BP
  - SI
  - DI

Registradores de segmento

- Não foram estendidos para 32 bits
- Informações sobre o código, dados, pilha
- Requerem muito cuidado quando alterados

Registradores de segmento

- Segment:offset
  - Espaço de endereçamento de 1MiB
  - (segment << 4) + offset
  - Vários endereços para cada segmento
  - Endereços repetidos e overflow
- O comando `ORG`

Principais Operações do NASM

- Load/Store: `mov`
- Lógicas: `xor,and,or`
- Aritméticos: `add,sub,inc,dec`
- Comparativas:`cmp,test`
- Saltos: `je,jne,jz,jnz,jmp`
- Pilha: `push,pop`
- Interrupção: `int`

Funcões e Macros

- Funções
  - `call` e `ret`
  - O código não se altera com a execução
- Macros
  - Sinal de `%`
  - Possui parâmetros
  - Altera o código assembly da mesma forma que o define em C

Funcões e Macros

- Macros
  - EX:

```
%macro prologue 1
   push ebp
   mov ebp,esp
   sub esp,%1
%endmacro
```

Interrupções

- Sinal que tipicamente resulta numa **troca de contexto**.
- Suspende temporariamente o que o processador está fazendo no momento de sua ocorrência
- Podem ser de hardware ou software, externas ou internas.

Interrupções no Linux

- Int 80h (0x80) = syscall
- Precisa de parâmetros
- EAX = tipo da syscall

```
;Hello,World!
section .text
global _start
_start:

mov eax,4
mov ebx,1
mov ecx,hello
mov edx,tam
int 80h

mov eax,1
mov ebx,0
int 80h
section .data
hello: db 'Hello, World!',0Ah
tam :equ $- hello ;
```

Compilando um programa

- Baixe o pacote nasm
- Escreva o código e salve como nome.asm
- No terminal:
  - Vá para a pasta onde se encontra o código
  - nasm -f elf nome.asm
  - ld -s -o nome nome.o

Interrupções da BIOS

- Registradores de 16 bits
- Vários tipos (int 10h, int 13h,int 16h...)
- AH = valor secundário da interrupção
- Outros registradores recebem os parâmetros

Compilando um programa

- Baixe o qemu e o nasm
- Escreva o código e salve como nome.asm
- No terminal:
    - Vá para a pasta onde se encontra o código
    - $nasm -f bin nome.asm -o nome.bin
    - $qemu nome.bin

Referências

- Helpcc - Interrupções da bios e comandos
- http://stanislavs.org/helppc/
- Scan Codes
- http://stanislavs.org/helppc/scan_codes.html
- Tabela de Syscalls
- http://bluemaster.iu.hio.no/edu/dark/lin-asm/syscalls.html
- TECH Help - Interrupções da bios
- http://webpages.charter.net/danrollins/techhelp/0002.HTM