Diskussion SW-Teil

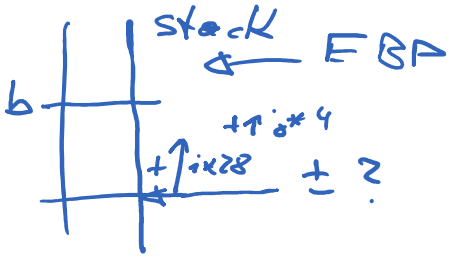
Dienstag, 2. Juli 2019 09:37

```
int a[5][7]; // global
int i,j;
  :
a[i][j] = 17; <->  mov EAX, DWORD PTR [i]
                   mov EBX, DWORD PTR [j]
                   imul EAX, 4*7
                   mov DWORD PTR [EAX+EBX*4+a], 17
```

Opcode — Basis-register — Index — Scale — disp! — immediate

```
int b[5][7]; // lokal

b[i][j] = 17;
```




```
b[i][j] = 17;
00E349F4 6B 05 38 91 E3 00 1C imul   eax,dword ptr [i (0E39138h)],1Ch
00E349FB 8D 8C 05 6C FF FF FF lea    ecx,b[eax]
00E34A02 8B 15 3C 91 E3 00    mov    edx,dword ptr [j (0E3913Ch)]
00E34A08 C7 04 91 11 00 00 00 mov    dword ptr [ecx+edx*4],11h
```

i*28 → eax

EBP ± ? + eax → ecx

j → edx

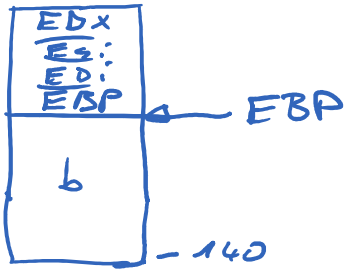
11h → ecx + edx*4

Gleiches Bsp.: _declspec (naked)

```
void lokarray(void) {
   int b[5][7];

   b[i][j] = 17;
}
```

Stackframe "naked"



Betrachtete Befehlsgruppen:

Zuweisung + Typkonversion

mov — FILD, FLD

movsx — FIST, FST

movzx

Arithmetik

add, sub — FADD, FSUB, FIADD, FISUB

mul, div, imul, idiv FMUL, FDiv, F.MUL, F.DIV

Vergleiche

cmp fcmp

Flags fstsw

Verzweigungen

JMP, Jcc (Betrag / 2-er Komp!)

Funktionen

push / pop

ret / call