



ความปลอดภัยคอมพิวเตอร์ (424)

Buffer overflow attack (1/2)

สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชาชีวกรรมคอมพิวเตอร์

กรงฤทธิ์ กิติศรีวงศ์พันธุ์

Email : songrit@npu.ac.th

สาขาวิชาชีวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนครพนม

Revised 2020-06-26

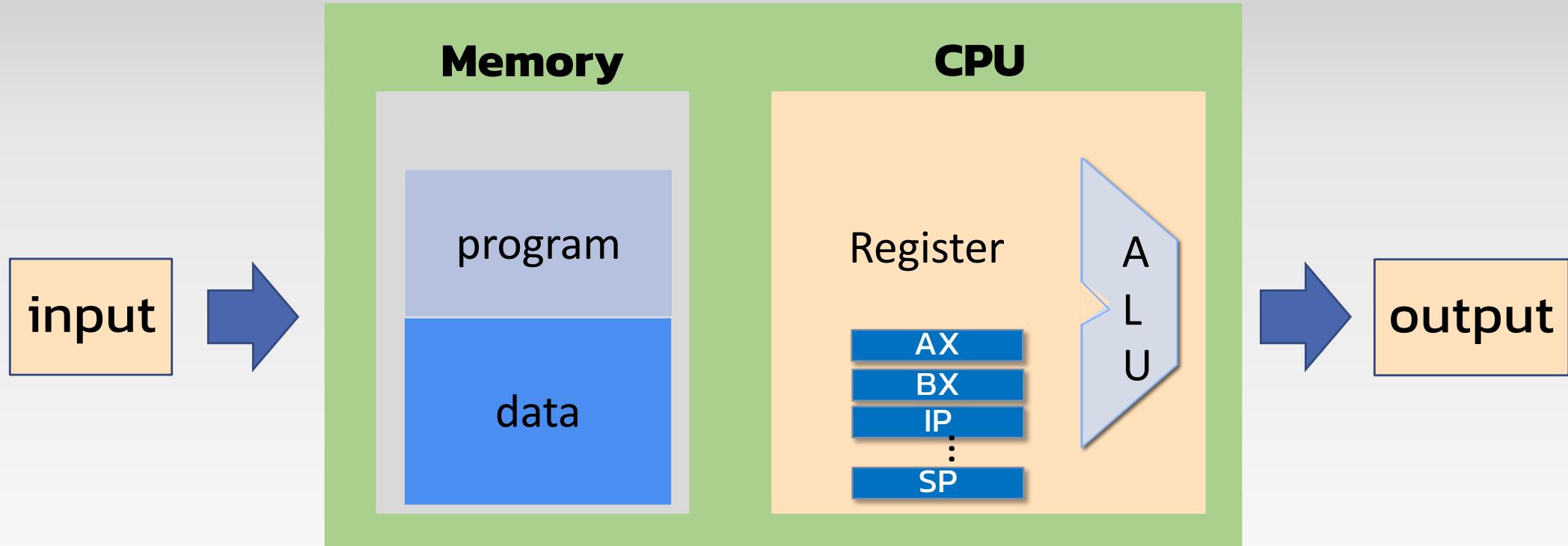
Lecture plan

- 1.1 ข้อมูลเบื้องต้น
- 1.2 ชนิดช่องโหว่ด้านความปลอดภัย
- 1.3 ชนิดการโจมตี
- 1.4 แรงจูงใจการโจมตีทางไซเบอร์
- 1.5 การโจมตี: Buffer overflow (1/2)

ຕັວຢ່າງ buffer overflow

- `/home/b5517550011/w3/overflow-2_wXUVuihkYcpFEPOfnQuuEJuRdlVmHR`
- <https://blog.rapid7.com/2019/02/19/stack-based-buffer-overflow-attacks-what-you-need-to-know/>

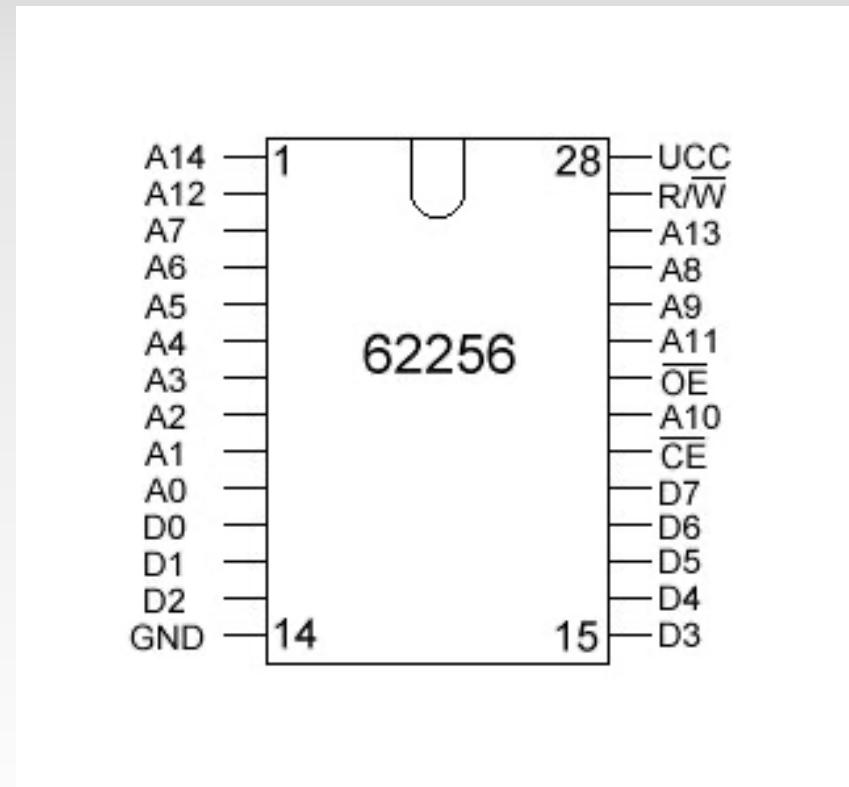
สถาปัตยกรรมฟ่อนอยมันนี



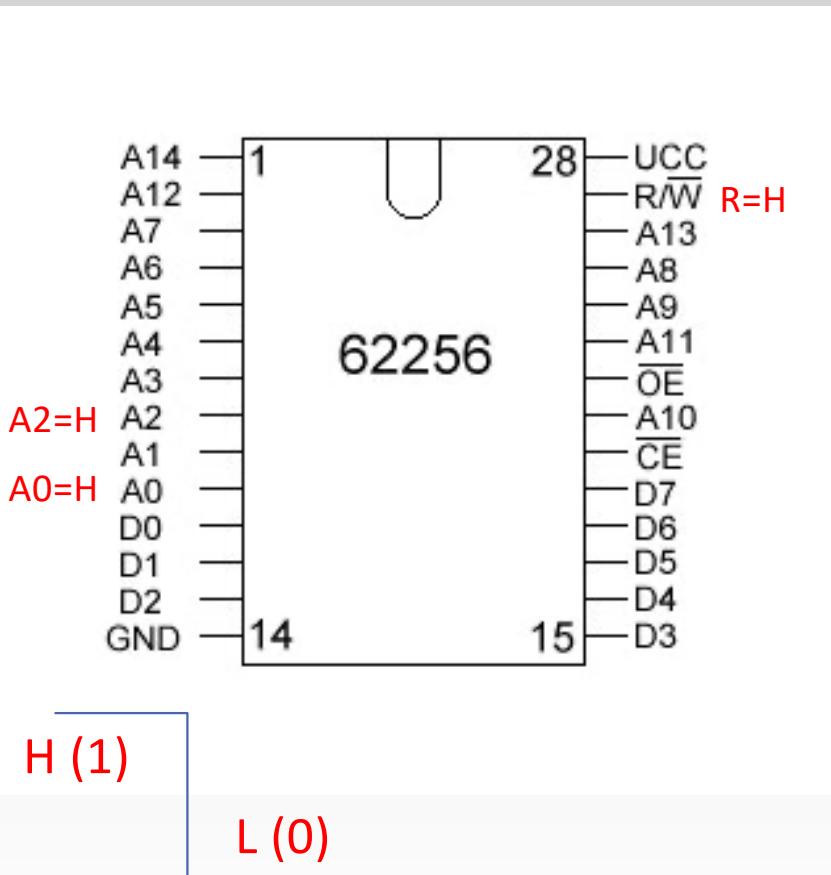
ระบบคอมพิวเตอร์

ຕັວອຍ່າງນໍ່ວຍຄວາມຈຳ (CY62256)

- 256-Kbit (32 K × 8) Static RAM

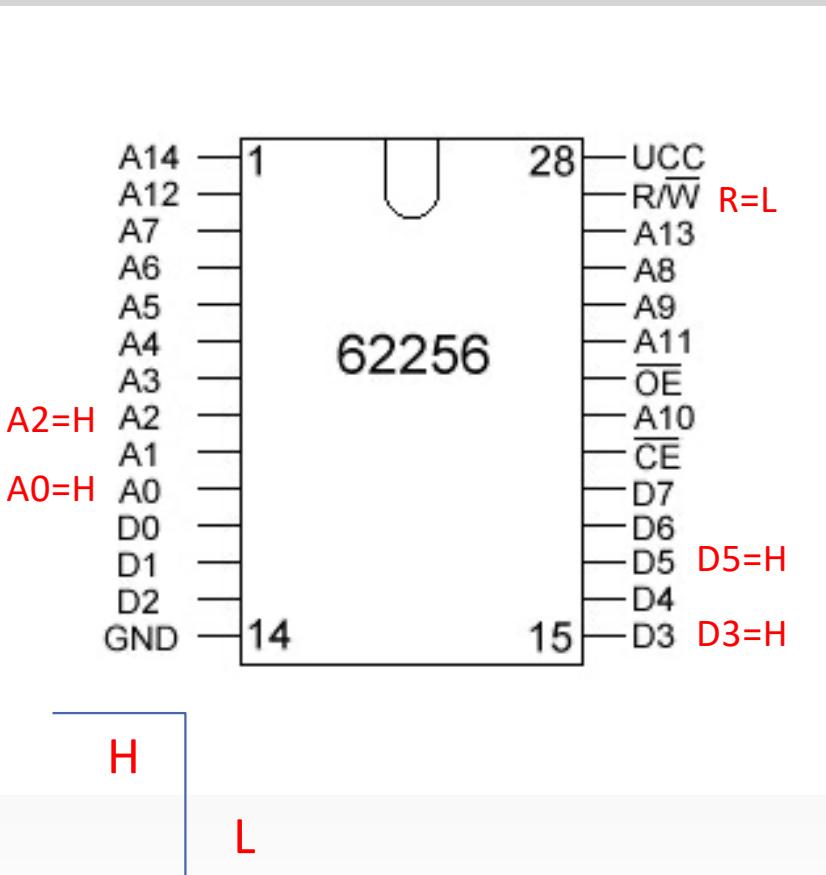


อ่านข้อมูล



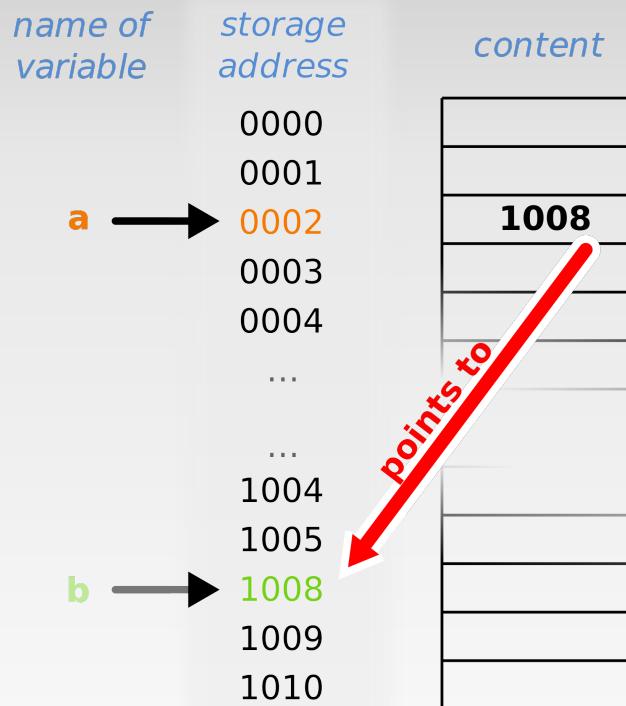
- อ่านข้อมูลที่ $addr = 0x0005$
 - $R=1$
 - $a_{15}a_{14} \dots a_2a_1a_0$
 - $A = (00000000 \ 00000101)_2$
 - $D[7..0] =$ ข้อมูลที่บันทึกใน RAM

ເບີຍນຫ້ວມູລ



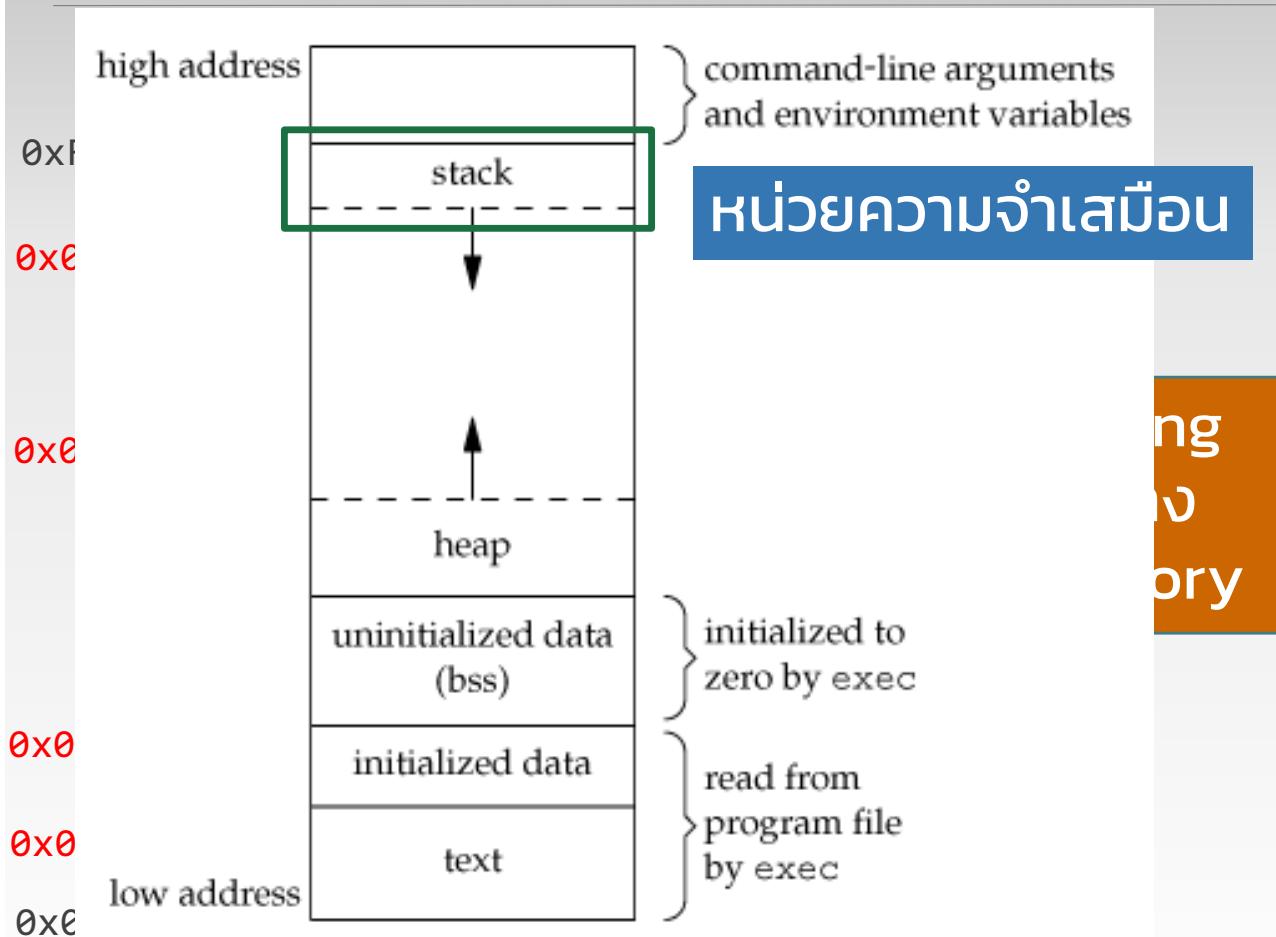
- ເບີຍນຫ້ວມູລທີ addr = $0x0005$
 - $a_{15}a_{14}\dots\dots\dots a_2a_1a_0$
 - $(00000000 \ 00000101)_2$
- ເບີຍນຫ້ວມູລ $0x06$ ທີ addr = $0x0005$
 - $R=0$
 - $d_7d_6\dots\dots d_1d_0 = (0010 \ 1000)_2$

ຮູບແບບນິຍມ ວິທາຍ memory



- ຄອນພິວເຕອນ 32ບັກ
- ອ່ານຂ້ອມຸລຈາກacenຍຄວາມຈຳຄັ້ງລະ 32ບັກ
- ອ່ານຂ້ອມຸລ address ລະ 4ໃບຕໍ່ (32ບັກ)

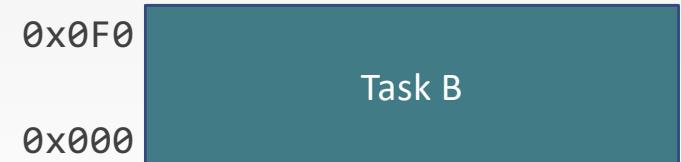
សេចក្តីយការណា



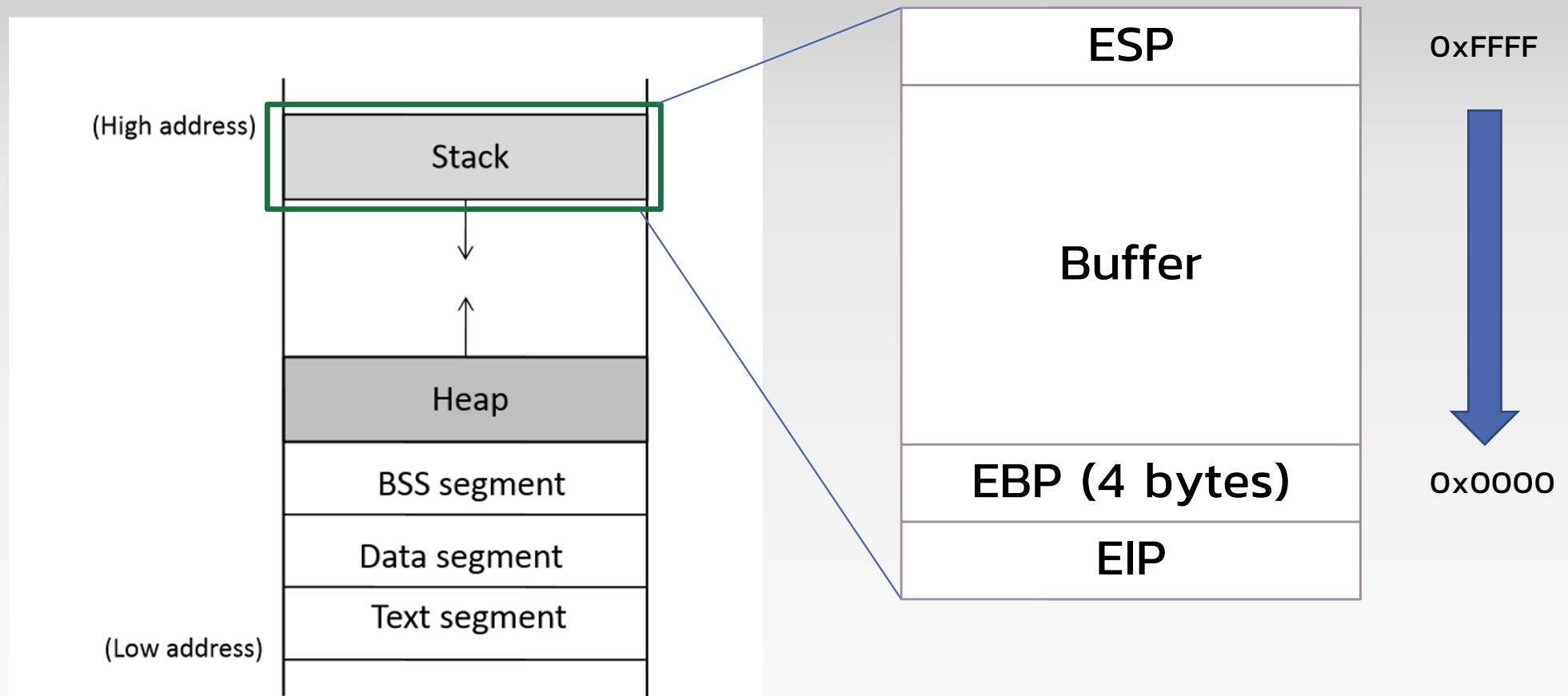
ប្រធែត 1



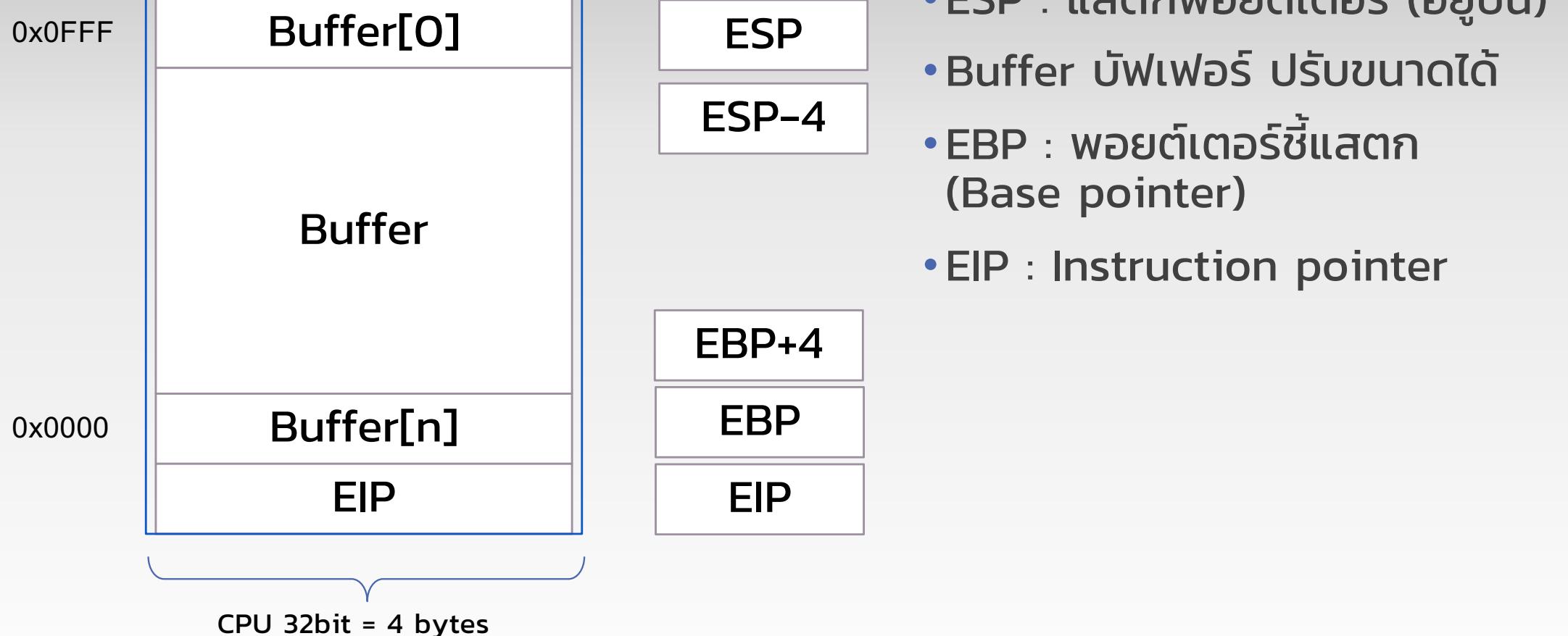
ប្រធែត 2



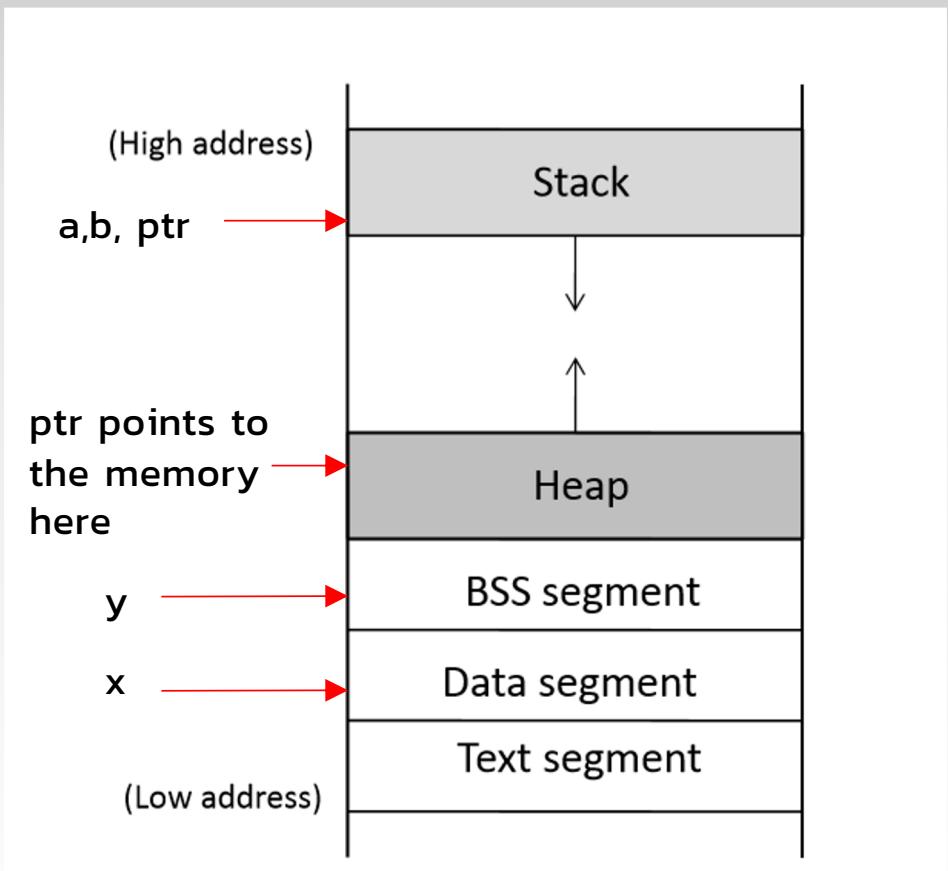
អប់យកគម្រោងផ្សេងៗ



Stack frame



អប់យកវារម៉ាសេម៉ូន



```
int x = 100;
int main()
{
    // data stored on stack
    int a=2;
    float b=2.5;
    static int y;

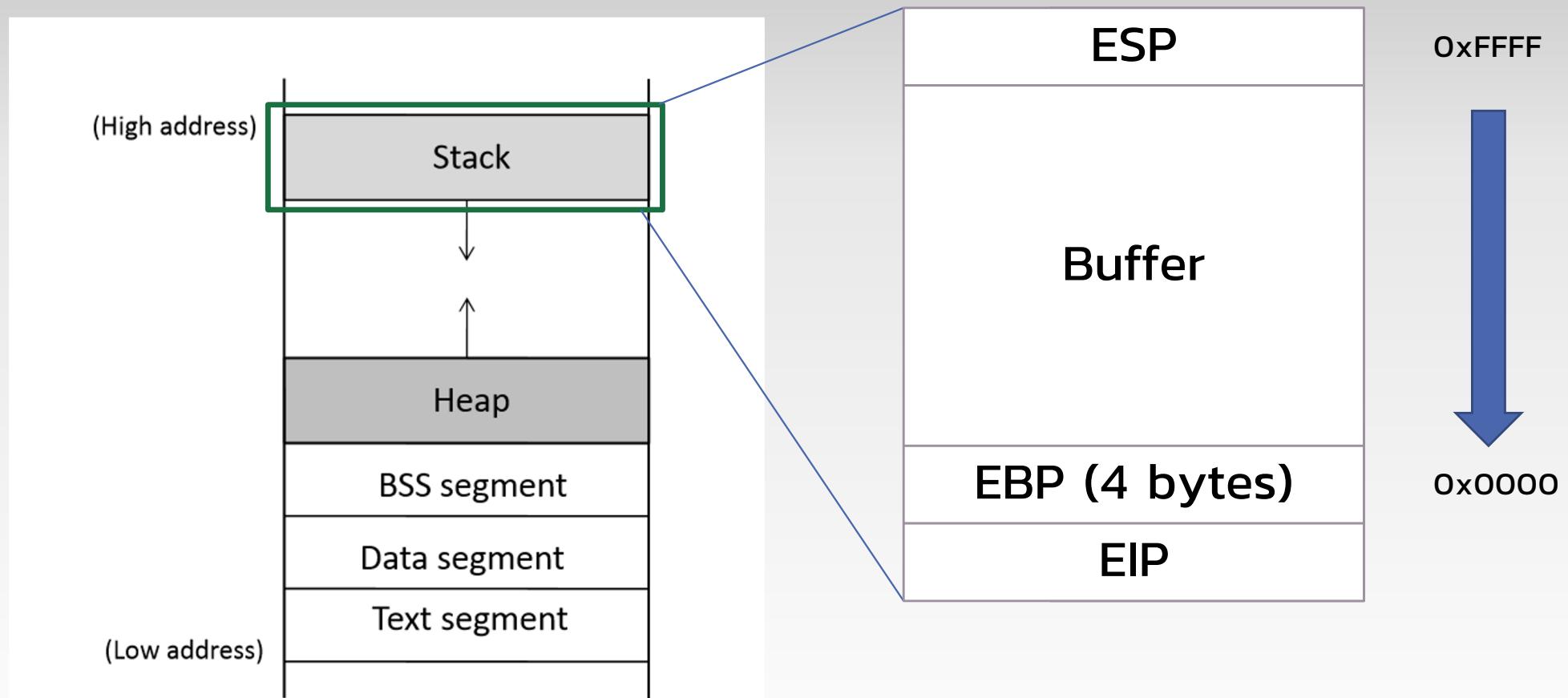
    // allocate memory on heap
    int *ptr = (int *) malloc(2*sizeof(int));

    // values 5 and 6 stored on heap
    ptr[0]=5;
    ptr[1]=6;

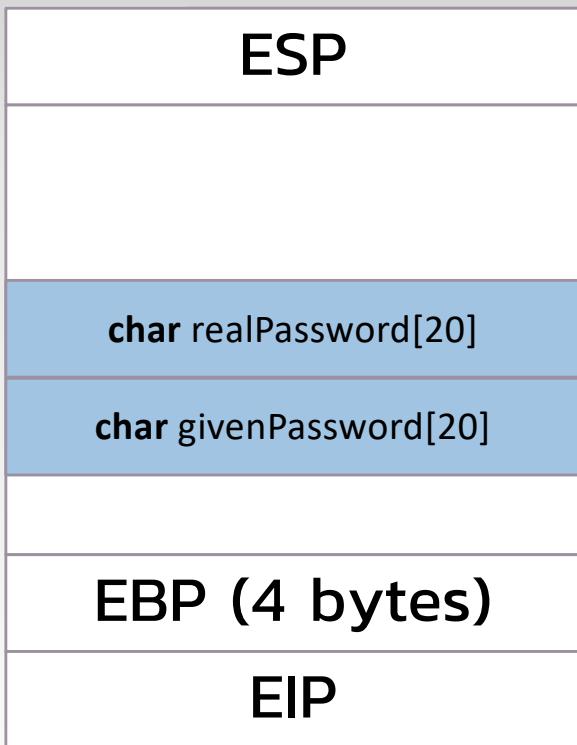
    // deallocate memory on heap
    free(ptr);

    return 1;
}
```

អប់យកគម្រោងផ្សេងៗ



bof.c



- if ($O == \text{strcmp}(\text{givenPassword}, \text{realPassword}, 20)$)

AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA

realPassword

givenPassword