



ความปลอดภัยคอมพิวเตอร์ (424)

Buffer overflow attack (1/2)

สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชา工กรรมคอมพิวเตอร์

กรงฤทธิ์ กิติศรีวงศ์พันธุ์

Email : songrit@npu.ac.th

สาขาวิชา工กรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนគរបเม

Revised 2020-06-26

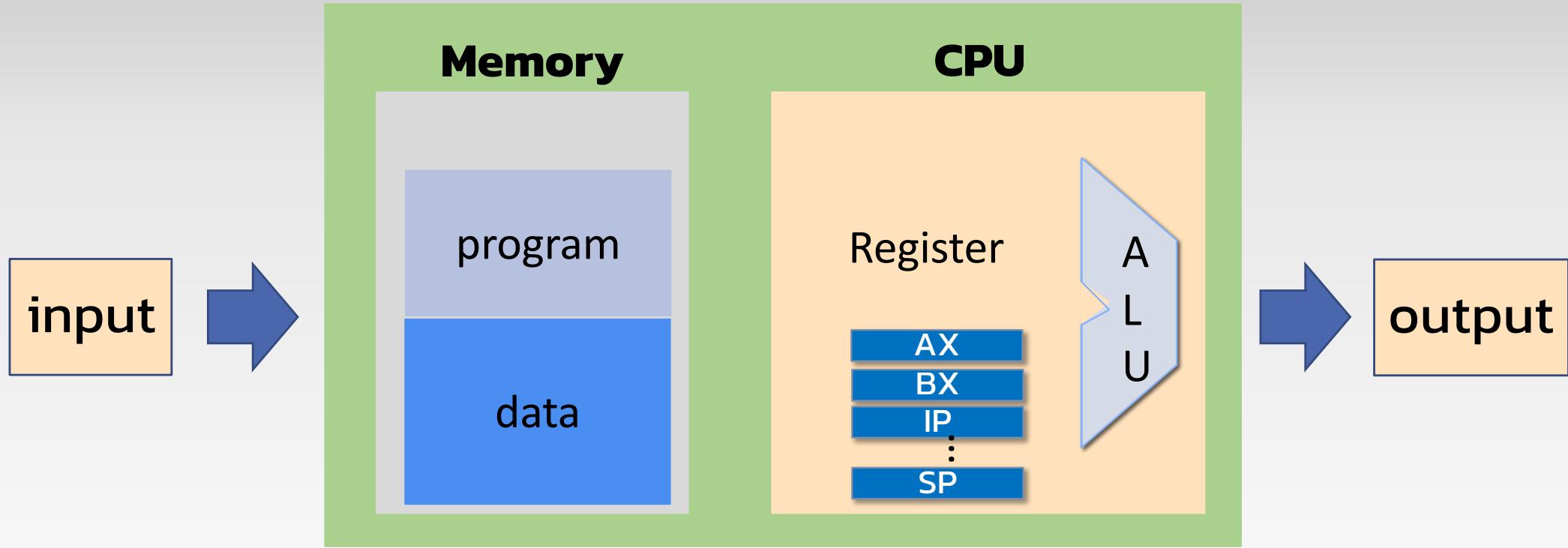
Lecture plan

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

ຕັ້ງວຍ່າງ 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/>

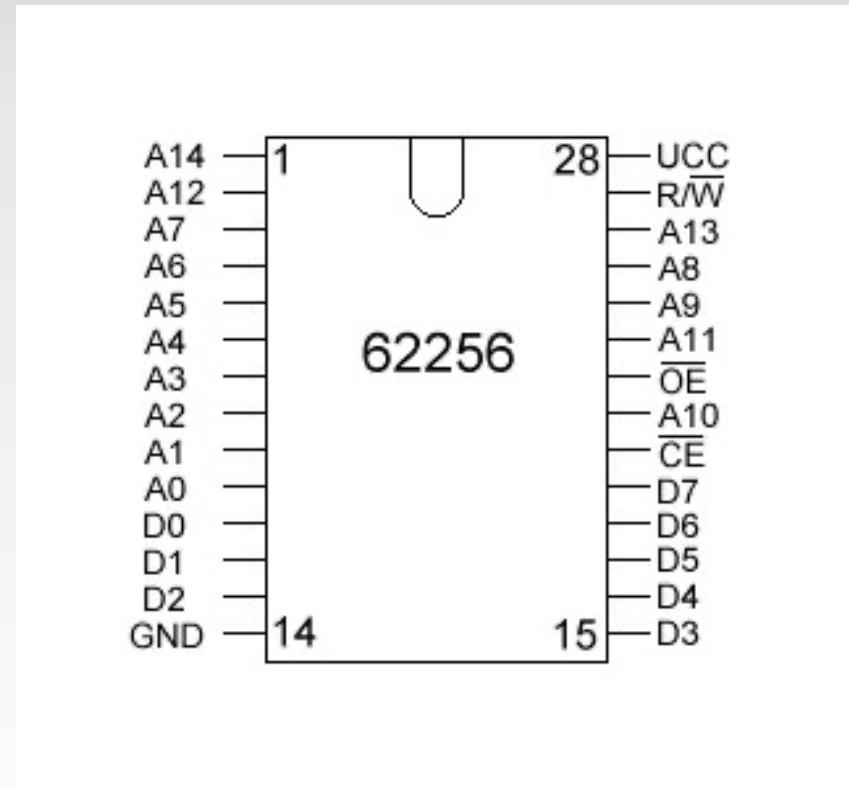
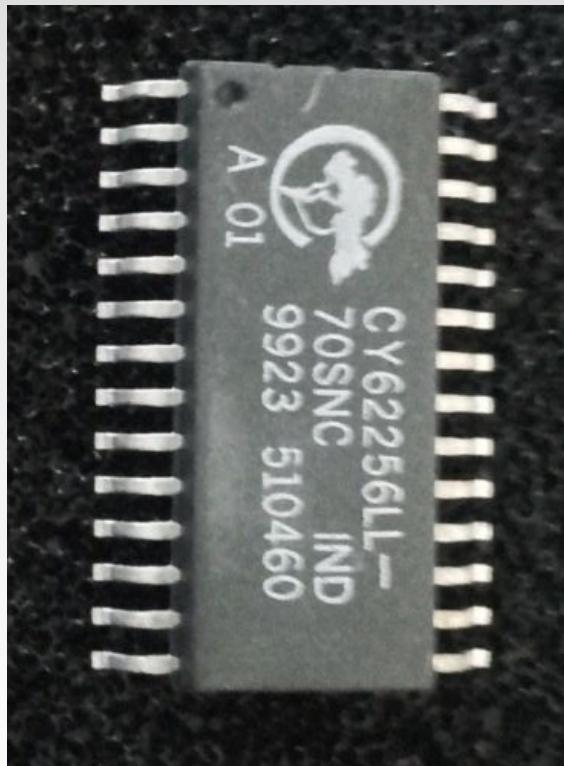
ສາປ້າຕຍກຣມພົວນອຍມັນບີ



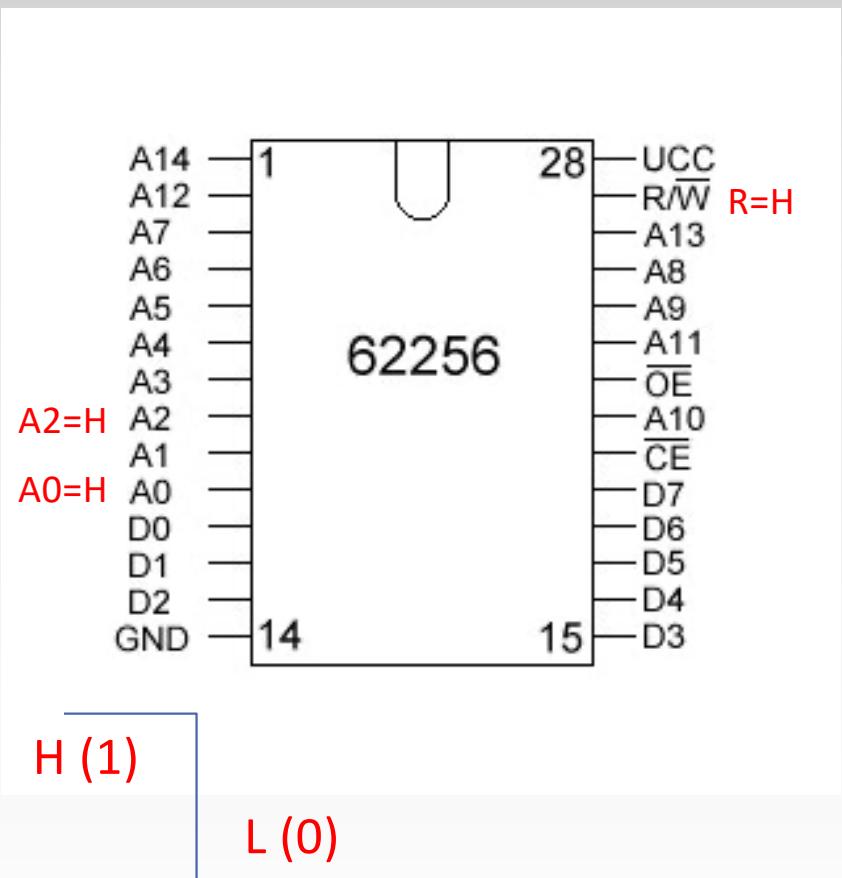
ຮະບັບຄອມພິວເຕອນ

ຕັ້ງຢ່າງນໍ່ຍຄວາມຈຳ (CY62256)

- 256-Kbit (32 K × 8) Static RAM

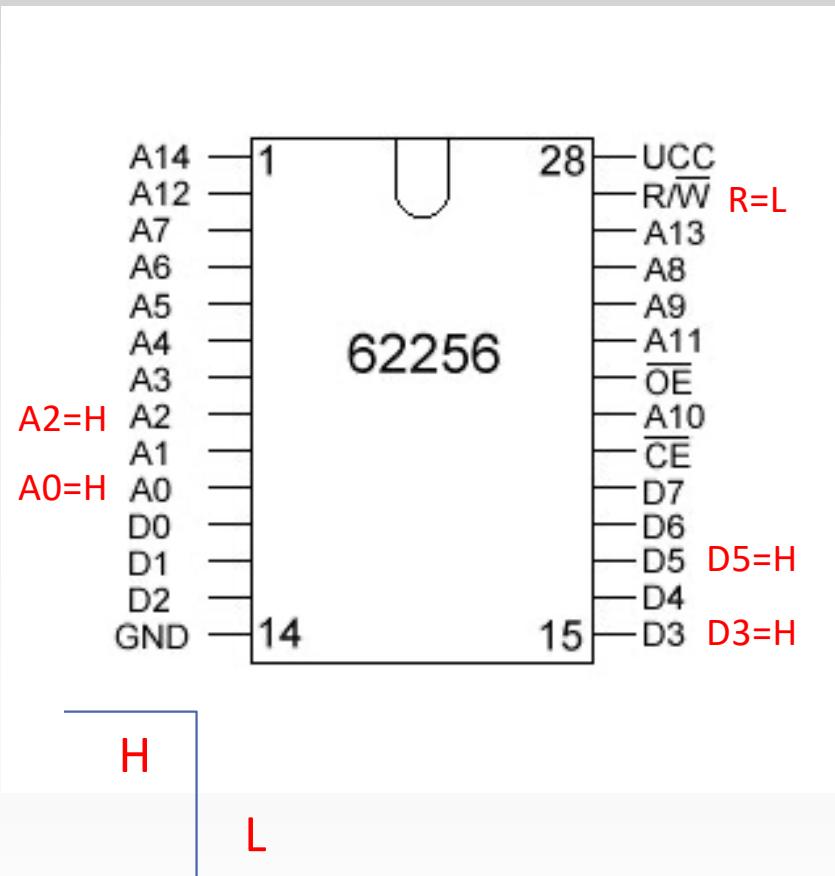


อ่านข้อมูล



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

ເບີຍບັນຫຸ່ມ



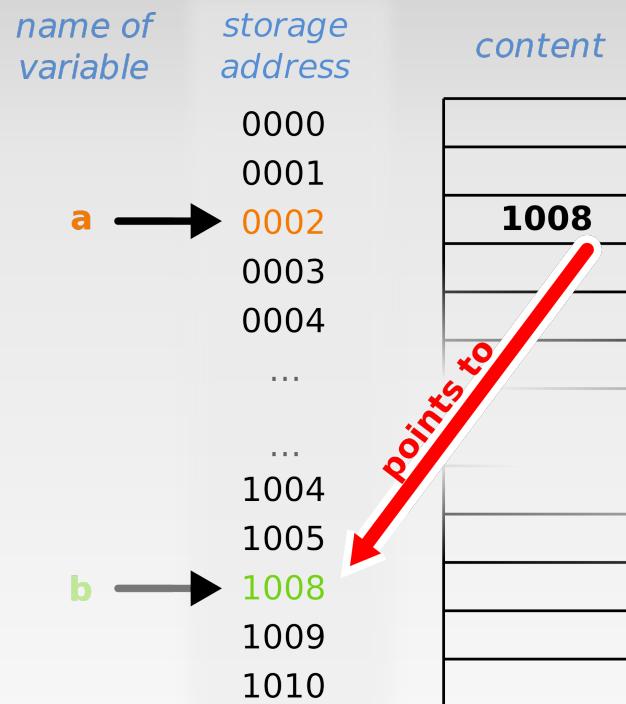
- ເບີຍບັນຫຸ່ມລືກ໌ addr = 0x0005

- $a_{15}a_{14}\dots a_2a_1a_0$
 - $(00000000 \ 00000101)_2$

- ເບີຍບັນຫຸ່ມ 0x06 ລືກ໌ addr = 0x0005

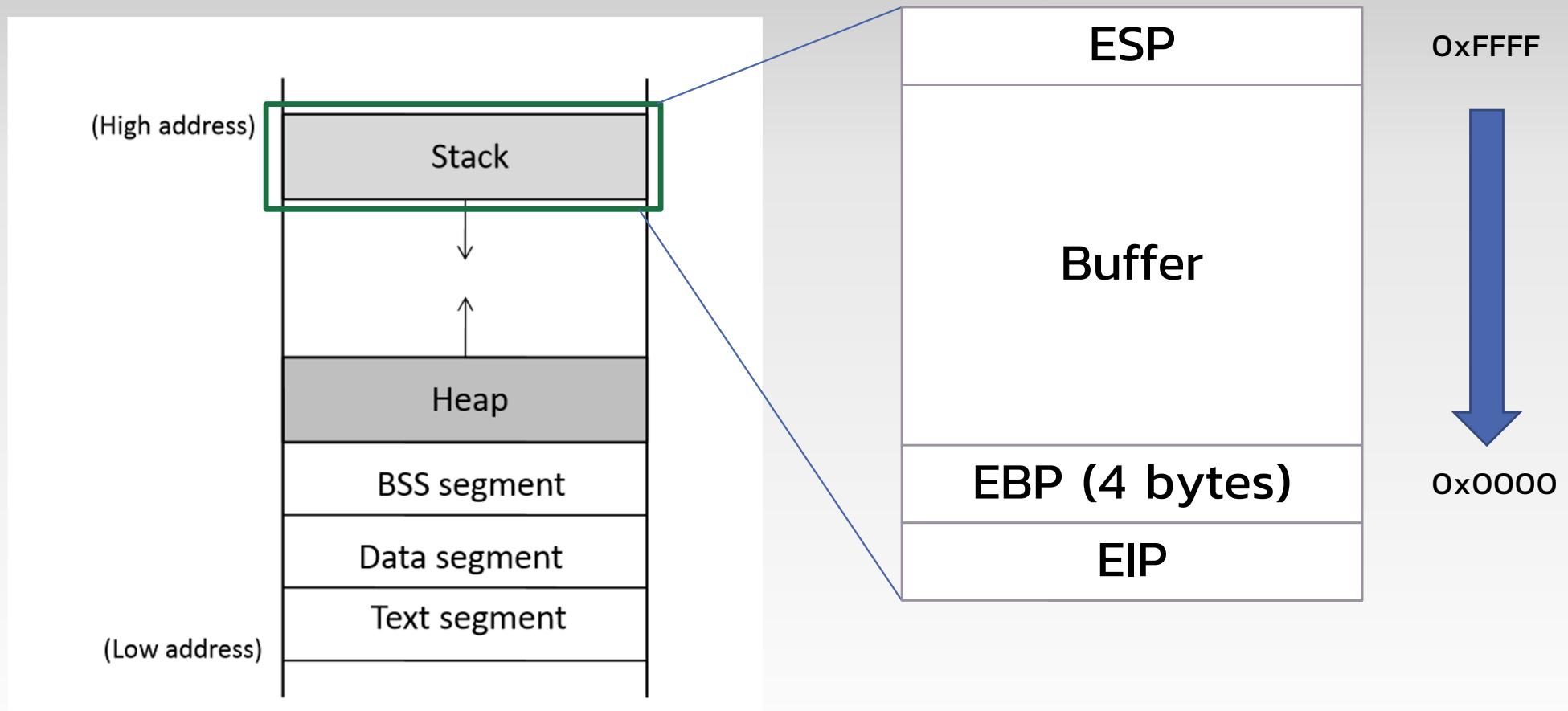
- $R=0$
 - $d_7d_6\dots d_1d_0 = (0010 \ 1000)_2$

ຮູບແບບນິຍມ ວິທາຍ memory

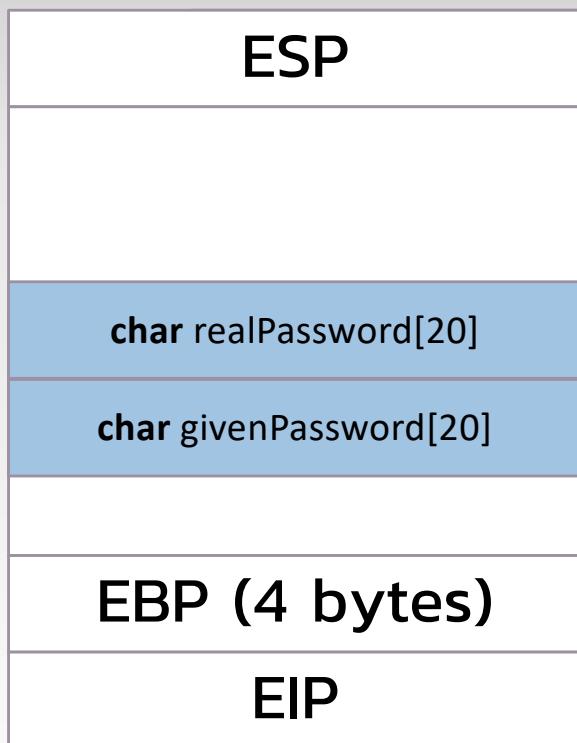


- ຄອນພົວເຕອນ 32ບັກ
- ອ່ານຂ້ອມຸລຈາກacenຍຄວາມຈຳຄັງຈະ 32ບັກ
- ອ່ານຂ້ອມຸລ address ລະ 4ໃບຕົວ (32ບັກ)

អប់យកគម្រោងផ្សេងៗ



bof.c



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

AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA

realPassword

givenPassword