המרכז
לחינוך סייבר
CYBER EDUCATION CENTER

Assembly for Reverse Engineering

Memory

Barak Gonen

לפני הכל

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- מינהלות
- פתרון תרגיל החולצות
- פתרון תרגיל zero regs

Subjects

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- What is physical memory?
- Why programs are loaded to RAM?
- What is the loader?
- How debuggers work?
- Hands on- using the .data section
- Special challenge – write code like malware does

Memory Wish List

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Large
- Cheap
- Fast
- Non Volatile
- Can’t have all in one…

  Hard Disk (HD) – Large, cheap, non volatile

  Random Access Memory (RAM) – Fast, volatile

  Cache (part of the CPU) – Ultra fast, very small

Physical Memory

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

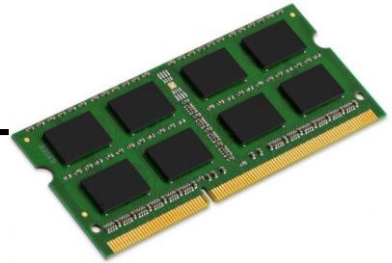
L1

Cache L2

Cache L3

RAM

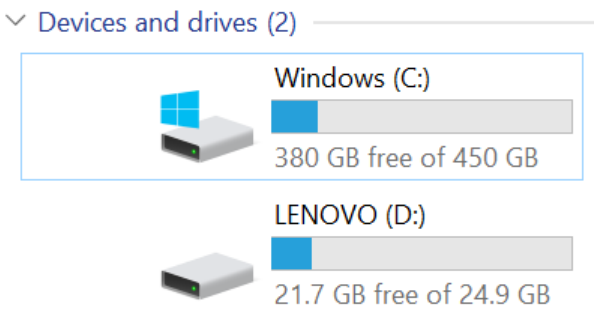
Hard Disk



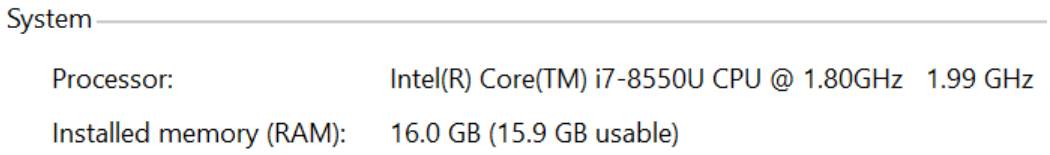
RAM vs HD: Size

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Hard disk size - use windows explorer



- RAM size – use control panel -> system &security -> system



RAM vs HD : Speed

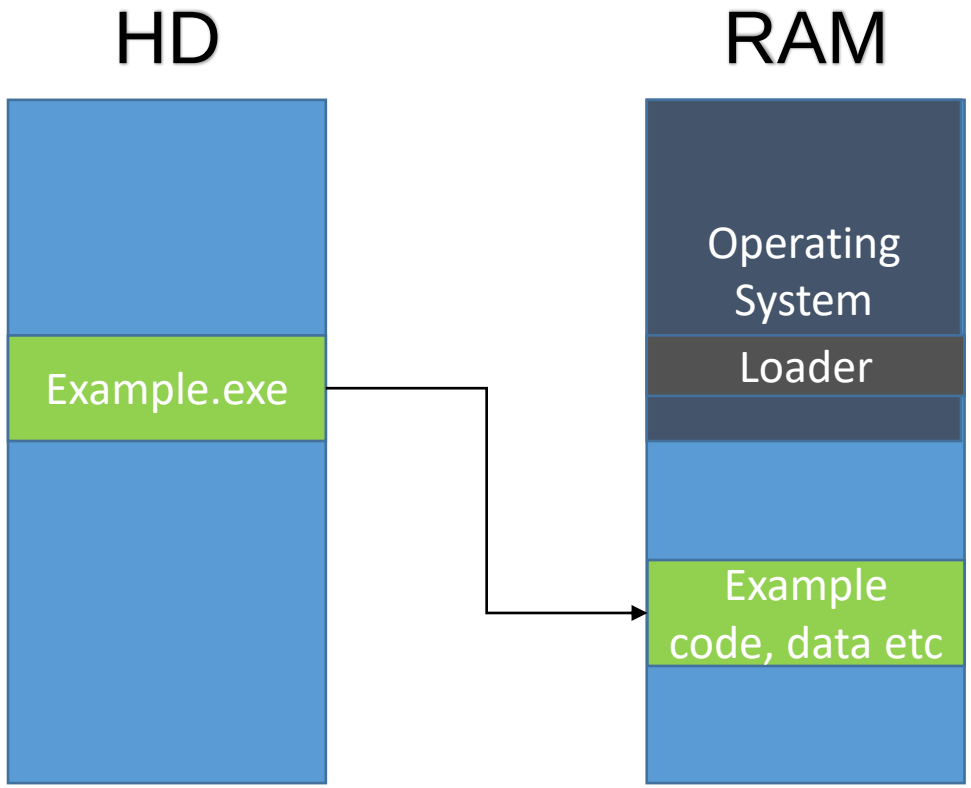
המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- CPU access to RAM: ~100ns
- CPU access to HD: ~1,000,000ns
- Why programs are running from RAM, not HD:
  - Imagine a 2GHz CPU waiting for HD…
  - HD memory is not 1-byte accessed

Loader

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Part of the operating system
- Purposes:
  - Loads EXE from HD to RAM
  - Sets EIP to start location
  - Changes addresses (optional)
  - Loads imports



How Debugger Works

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Step 1: User clicks on debugger
- Step 2: Debugger is loaded to RAM
- Step 3: User selects EXE to debug
- Step 4: Debugger opens sub-process with EXE name as parameter
- Step 5: Loader loads debugged EXE to RAM
- Trick: Debugger places special opcode on sub-process's RAM where breakpoints reside (opcode CC)

Wait a Minute…

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Can a Process know that it is being debugged?
- Very important for malware

Memory

המרכז
לחינוך סייבר
CYBER EDUCATION CENTER

- Each BYTE has a memory location
  - Byte- 8 bits
  - Word – 2 bytes
  - Double word – 4 bytes
- In 32 bit architecture, each memory reference may refer to a byte, a word or a double word

Defining Variables in Memory

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- db – define byte
- dw – define word
- dd – define double
- Value can be initialized:
- …Or not initialized:

```
my_var db 7
my_other_var db ?
```

Little Endian

- How ‘number’ is stored in memory?

```
section '.data' data readable writeable
    number  dd   0x6789ABCD
```

- Little Endian: Significant bytes stored in higher memory address

Address	Hex dump							
00401000	CD	AB	89	67	00	00	00	00
00401008	00	00	00	00	00	00	00	00

Defining Special Variables

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Defining an array:
  - DUP means ‘duplicate’

```
my_array db 5 dup(0x01)
```

- Defining a string:
  - 13 means ‘\r’
  - 10 means ‘\n’

```
my_str  db  'Hello class!',13,10
```

Defining Variables – cont.

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- What will be the memory map if the following variables were defined?
- Try it!

```
section '.data' data readable writeable
    a       dd   3
            db   0x65, 0x43, 0x21
    b       dd   3
            db   3 dup(0xff)
    result  dd   ?
            db   20 dup(?)
```

Accessing memory

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- The address is highly required ☺
- We use [ ] to indicate the value which is stored at the given address
- Direct memory address:
  - [0x04001000]
  - [var1] – when var1 is defined in data segment
- Indirect addressing:
  - [ebx] – if ebx is storing the address
  - [ebx + const] – fixed offset
  - [ebx + esi] – great for looping on arrays

Exercises – Memory

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

1. Define x to hold the value “8” in a byte size
2. Copy the value of x to AL
3. Copy the value at address 0x00401000 to AH
4. Copy the address of x to EBX
5. Define y to hold the value “9” in a byte size
6. Copy the value of [ebx] to CL
7. Copy the value of [ebx+1] to CH
8. Attempt to copy the value of x to AX
9. Attempt to copy the value at 0x00402000 to DL

Exercise – Your Name

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- https://data.cyber.org.il/reversing/name.pdf

Exercise – Possible

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- https://data.cyber.org.il/reversing/possible.pdf

Homework – Secret Message

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- https://data.cyber.org.il/reversing/whoRU.asm


QUESTIONS