Inline Programming with Assembly

By Milad Kahsari Alhadi

Last Update: Wednesday - 2019 24 April

- **Inline Programming with Assembly – 265 Min**
  - Introduction to Assembly
    i. Different Processors and Assembly
       1. MIPS
       2. Intel
       3. Arm
       4. Machine Language
  - Processor Architectures
    i. System Organization Basic
       1. Central Processing Unit
       2. x86-x64 CPU Registers
       3. x86-x64 Segment Registers
       4. x86-x64 CPU Flags
       5. x86-x64 FPU Registers
    ii. CPU Mode
       1. Real Mode
       2. Protected Mode
       3. SMM Mode
       4. Long and Compatibility Mode
    iii. CPU Memory Models
       1. Flat Model
       2. Segmented Model
    iv. Process Image in Memory
       1. Flat
       2. Virtual
    v. Assembly Syntax
       1. Intel
       2. Att
  - Compilation and Linking Process
    i. Compilers:

1. Gnu Assembler – GAS
2. Flat Assembler – FASM
3. Netwide Assembler – NASM
4. High Level Assembler – HLA
5. Microsoft Assembler – MASM

ii. Linkers:
1. GNU Linker – LD Program
2. Microsoft Linker – MD Program

iii. Executabling:
1. 1st Phase: Assembling
2. 2st Phase: Linking

iv. File Format:
1. Executable Portable File Format – PE
2. Linkable and Executable File Format – ELF

– Principles of Assembly in x86-x64 Linux

i. Data Types:
1. NASM
2. MASM
3. GAS

ii. Procedures:
1. NASM
2. MASM
3. GAS

iii. Interface Programming:
1. Linux System Call Index
2. Windows System Call Index
3. System Call Handler – Interrupts
4. System Call Handler – Sysenter

iv. Common Instruction:
1. ADD, SUB, MUL and DIV
2. MOV, MOVB, MOVW and MOVS
3. PUSH, POP, PUSHA and POPA
4. RET, RETN and LEAVE
5. JMP and JXX
6. ...

v. Stack Memory Layout

vi. Change OEP

vii. ENT, EOT, EAT, IAT and Dlls
viii. Debuggers and Disassemblers:
    1. Hopper
    2. IDA
    3. GDB
    4. Visual Studio
    5. Radare2