REVERSE ENGINEERING

IDA OR GHIDRA ?

ABOUT ME

Manish Sharma

Security Engineer (3+ yrs)

Victoria’s Secret & Co.

Github - sh377c0d3

Twitter/LinkedIn - sh377c0d3

- This entire talk is more at personal level and doesn't contain or relate to any of my former or current professional associations.

- All content has been sourced from publicly available sources like the internet. The presenter does not infringe or claim rights over any content, images and any other work being presented here, and all rights belong to respective owners only.

LESS ON THEORY

MORE ON DEMO

- What is Reverse Engineering
- Exploit Development = Reverse Engineering ?
- Demo: IDA or Ghidra ?
- Conclusion & References
- Q & A

WHAT IS REVERSE ENGINEERING

- Understanding of the internals of
  - Something made by a human
  - Through analysis
  - Without having access to its design principles
  - The way its components interact with them in order to make it work

- In other words, it's the process of taking apart something that someone else built and understanding how he/she did it, partially or completely.

WHAT IS REVERSE ENGINEERING (CONTD.)

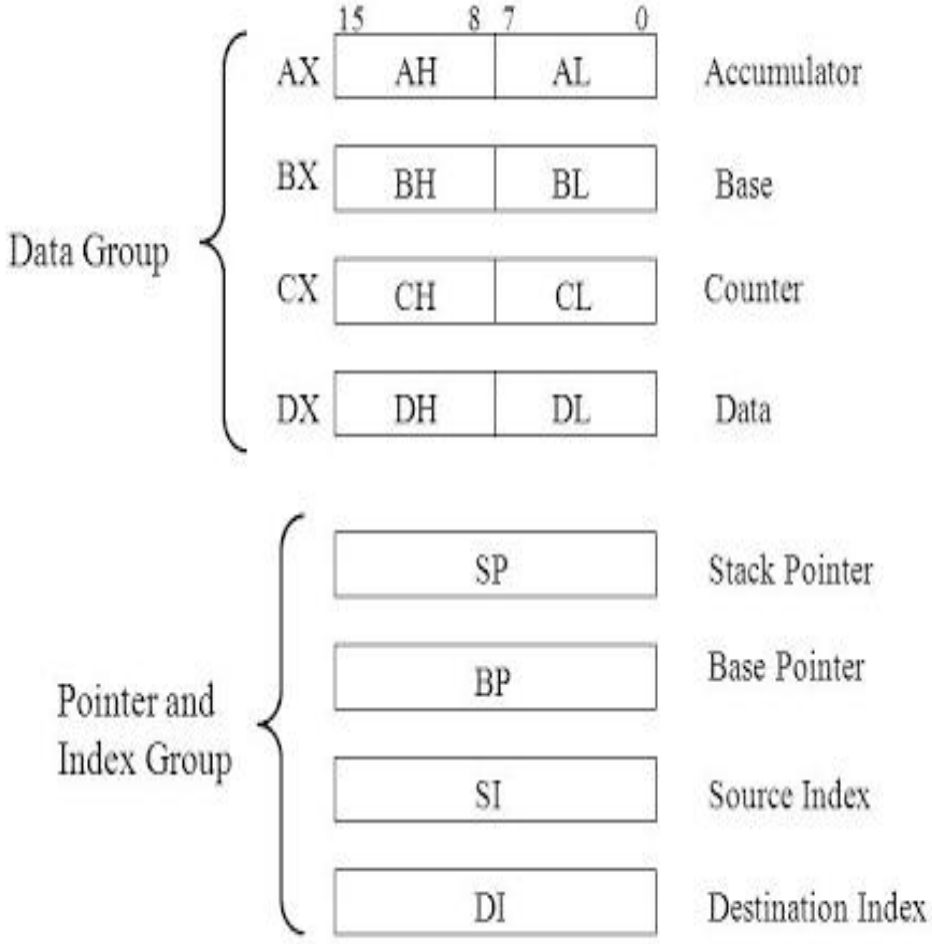
- Things to know before we dive in:
  - Intel IA-32 CPU architecture (x86)
  - The stack
  - The heaps
  - As well as exceptions
  - Windows APIs with some Windows Internals
  - Most common types of reversing tools used these days.

- During the first steps in the world of reversing we will be dealing with behavioral observations regarding the execution of an application and how it reacts (or not) to our inputs.

The most important and necessary first step

is to manage to locate the algorithm(s)

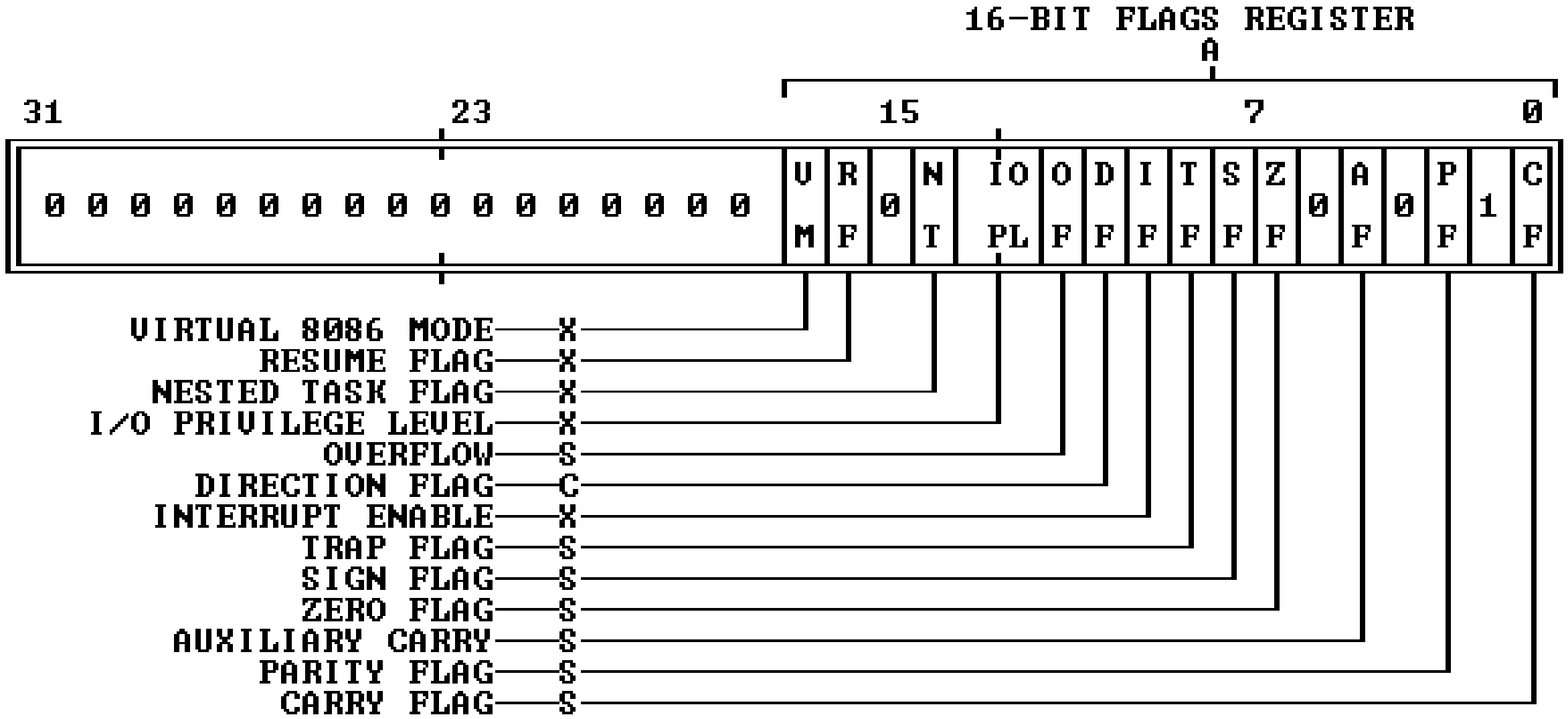
1. General Purpose Registers



General-Purpose Registers

31 16	15 8	7 0	16-bit	32-bit
	AH	AL	AX	EAX
	BH	BL	BX	EBX
	CH	CL	CX	ECX
	DH	DL	DX	EDX
	BP			EBP
	SI			ESI
	DI			EDI
	SP			ESP

Figure 2-8. EFLAGS Register



S = STATUS FLAG, C = CONTROL FLAG, X = SYSTEM FLAG

NOTE: 0 OR 1 INDICATES INTEL RESERVED. DO NOT DEFINE

```
; ------------------------------------------------------------------------
; Writes "Hello, World" to the console using only system calls. Runs on 64-bit Linux only.
; To assemble and run:
;
;     nasm -felf64 hello.asm && ld hello.o && ./a.out
; ------------------------------------------------------------------------

          global    _start

          section   .text
_start:   mov       rax, 1                  ; system call for write
          mov       rdi, 1                  ; file handle 1 is stdout
          mov       rsi, message            ; address of string to output
          mov       rdx, 13                 ; number of bytes
          syscall                           ; invoke operating system to do the write
          mov       rax, 60                 ; system call for exit
          xor       rdi, rdi                ; exit code 0
          syscall                           ; invoke operating system to exit

          section   .data
message:  db        "Hello, World", 10      ; note the newline at the end
```


IF YOU KNOW ASSEMBLY
EVERY SOFTWARE
IS OPEN SOURCE
imgflip.com

EXPLOIT DEVELOPMENT = REVERSE ENGINEERING ?

When it's been 7 hours and you still can't understand your own code

EXPLOIT DEVELOPMENT = REVERSE ENGINEERING ?

CONCLUSION & REFERENCES

- Never Limit yourself to single tool or technique
- IDA Pro is good but Ghidra is awesome too
- Don't forget to check other open-source tools
- Understanding of Basics is must
- At last … here are few reference that might help you:
  - https://0xinfection.github.io/reversing/
  - https://geoffchappell.com/index.htm?ta=10.60000228881836
  - https://htmlpreview.github.io/?https://github.com/NationalSecurityAgency/ghidra/blob/stable/GhidraDocs/CheatSheet.html
  - https://www.hex-rays.com/products/ida/support/freefiles/IDA_Pro_Shortcuts.pdf
  - https://static.grumpycoder.net/pixel/docs/GhidraClass/Beginner/Introduction_to_Ghidra_Student_Guide_withNotes.html#Introduction_to_Ghidra_Student_Guide.html


Thank You
Obrigado
Asante
Merci
Arigato
Kiitos
Mamana
GRAZIE
Juspaxa
MATONDO
Kia Ora
Vinaka
Salamat
NIRRINGRAZZJAK
Matondo
MAAKE
SPASIBO
Multumesc
Mochchakkeram
Raibh Maith Agat
Terma Kasih
Ua Tsaug Rau Koj
Cam on ban
DANK JE
Obrigado
Chokrane
Matur Nuwun