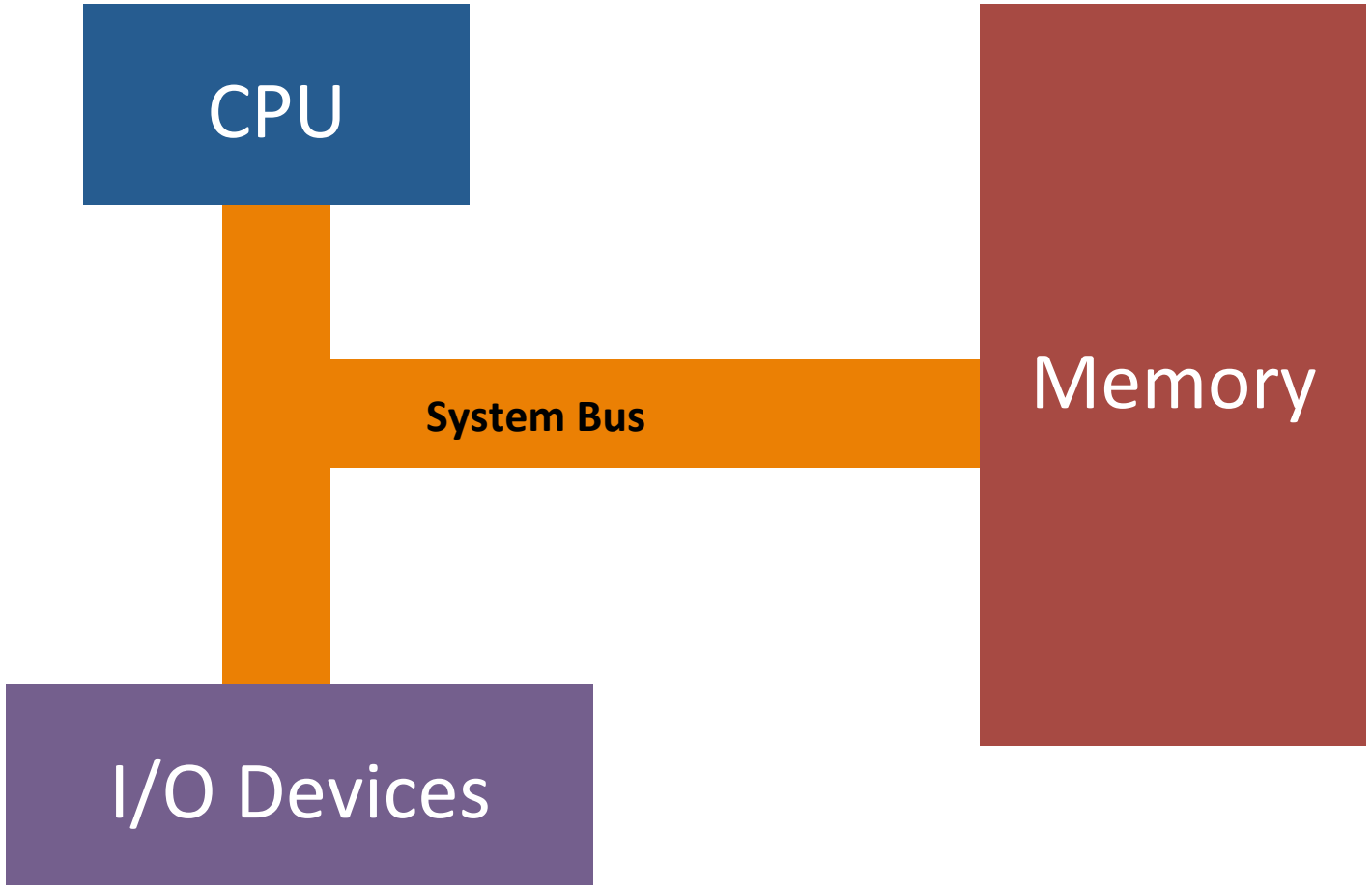
Module 1: 64-Bit ASM on Linux

4. CPU Registers

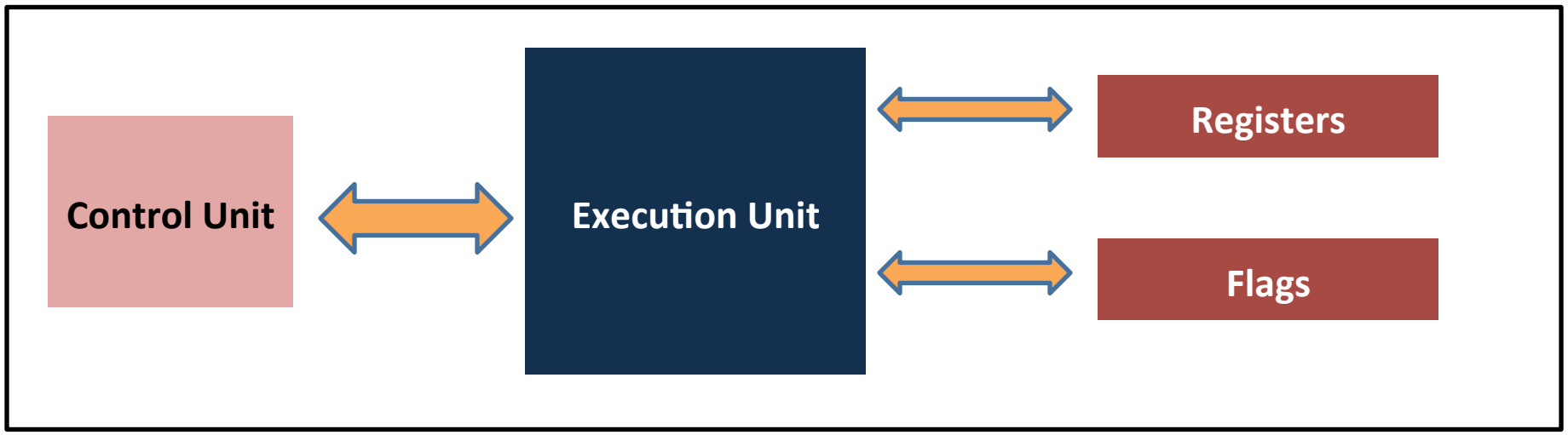
Vivek Ramachandran
SWSE, SMFE, SPSE, SGDE, SISE, SLAE^{64}, SLAE^{32} Course Instructor

http://SecurityTube-Training.com

System Organization Basics

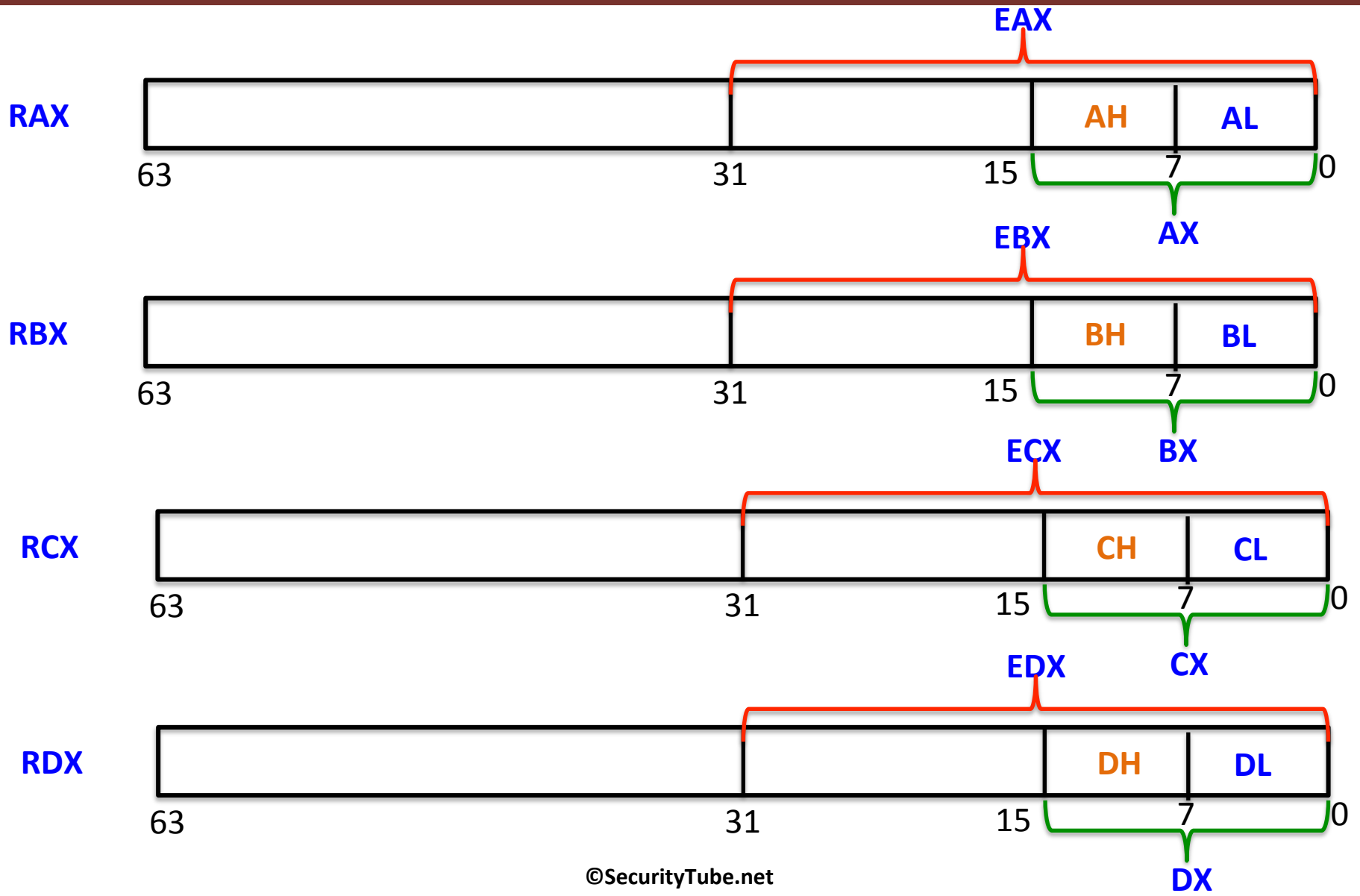


CPU

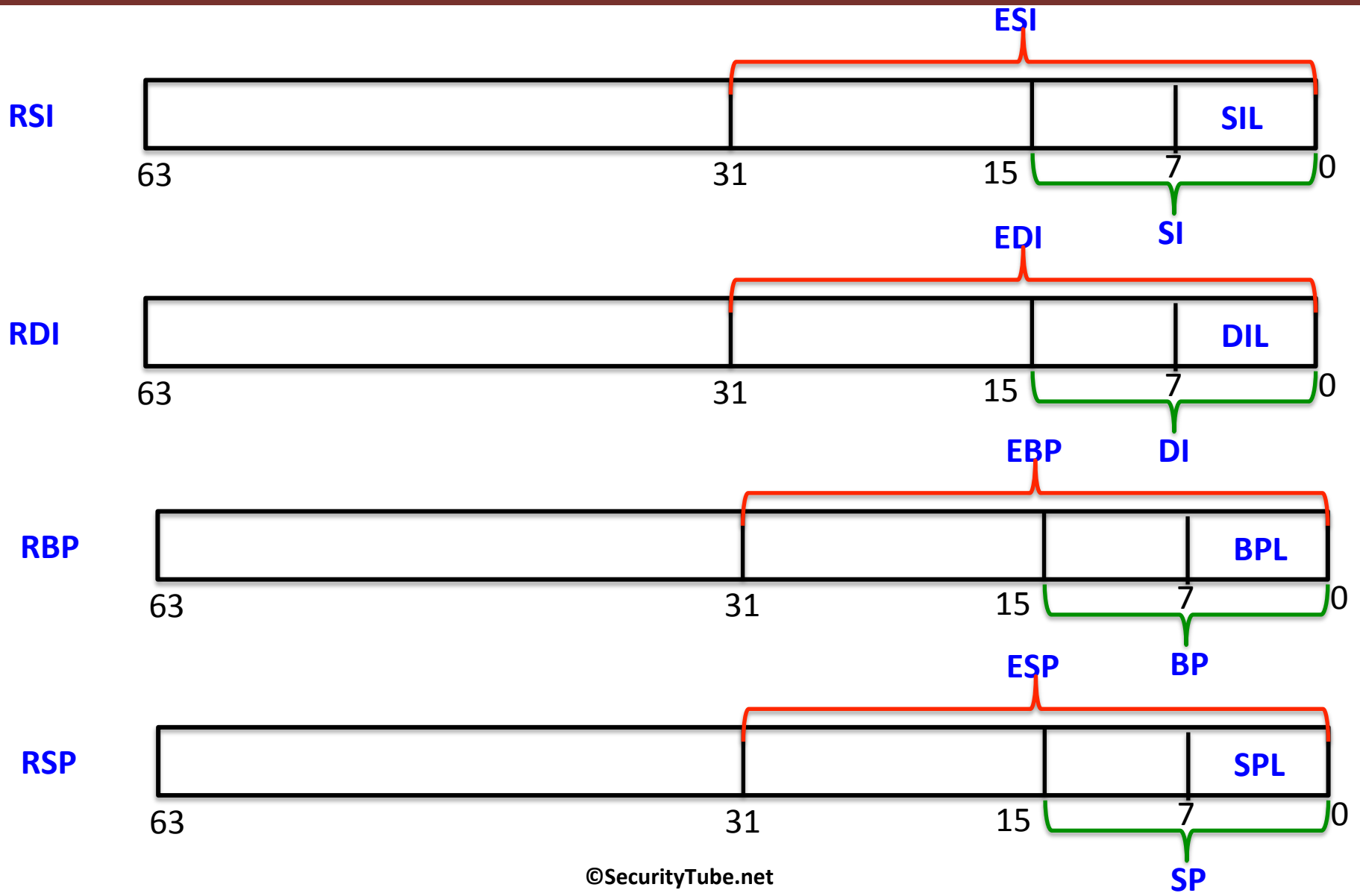


- **Control Unit** – Retrieve / Decode instructions, Retrieve / Store data in memory
- **Execution Unit** – Actual execution of instruction happens here
- **Registers** - Internal memory locations used as “variables”
- **Flags** – Used to indicate various “event” when execution is happening

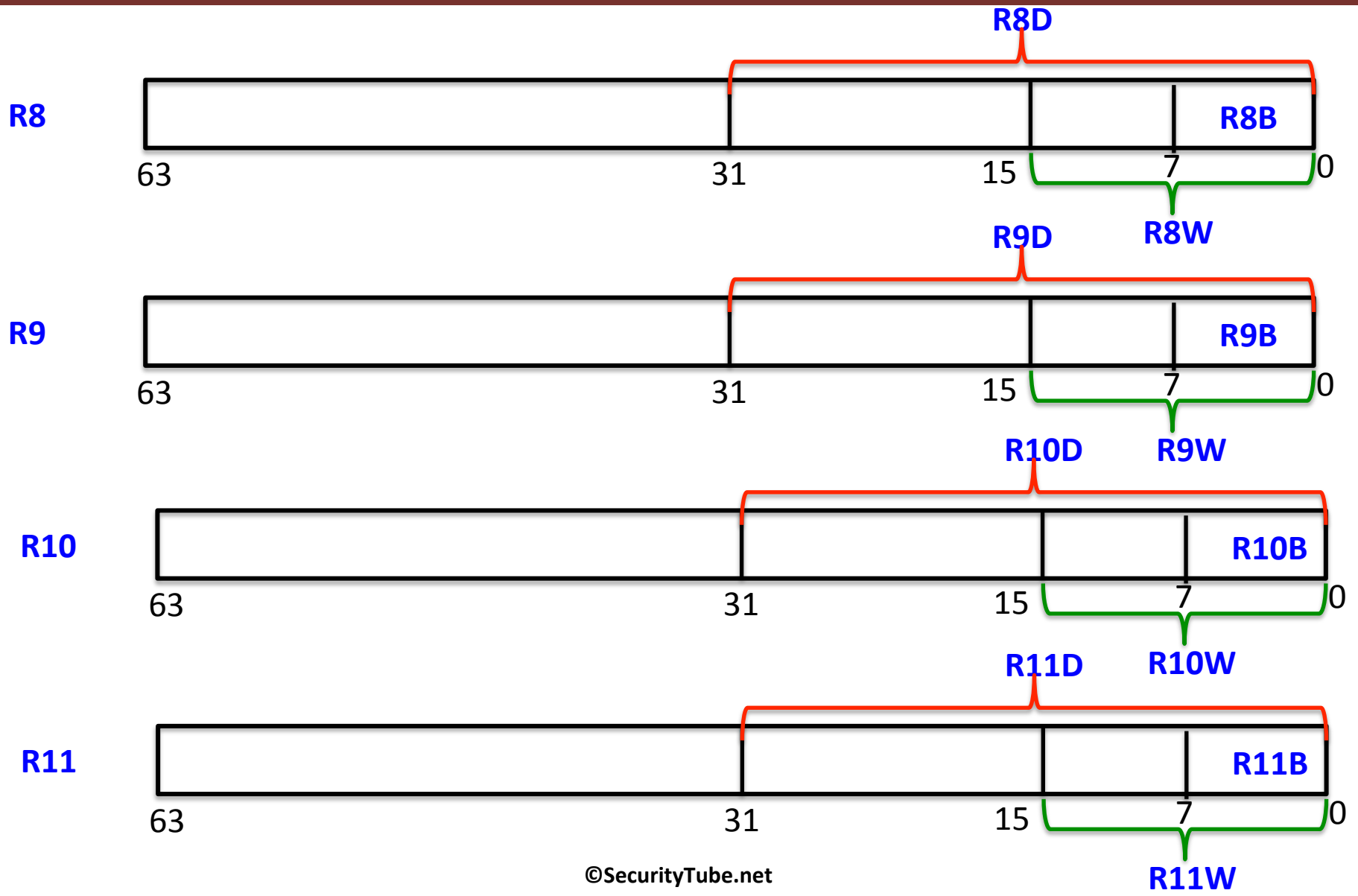
General Purpose Registers



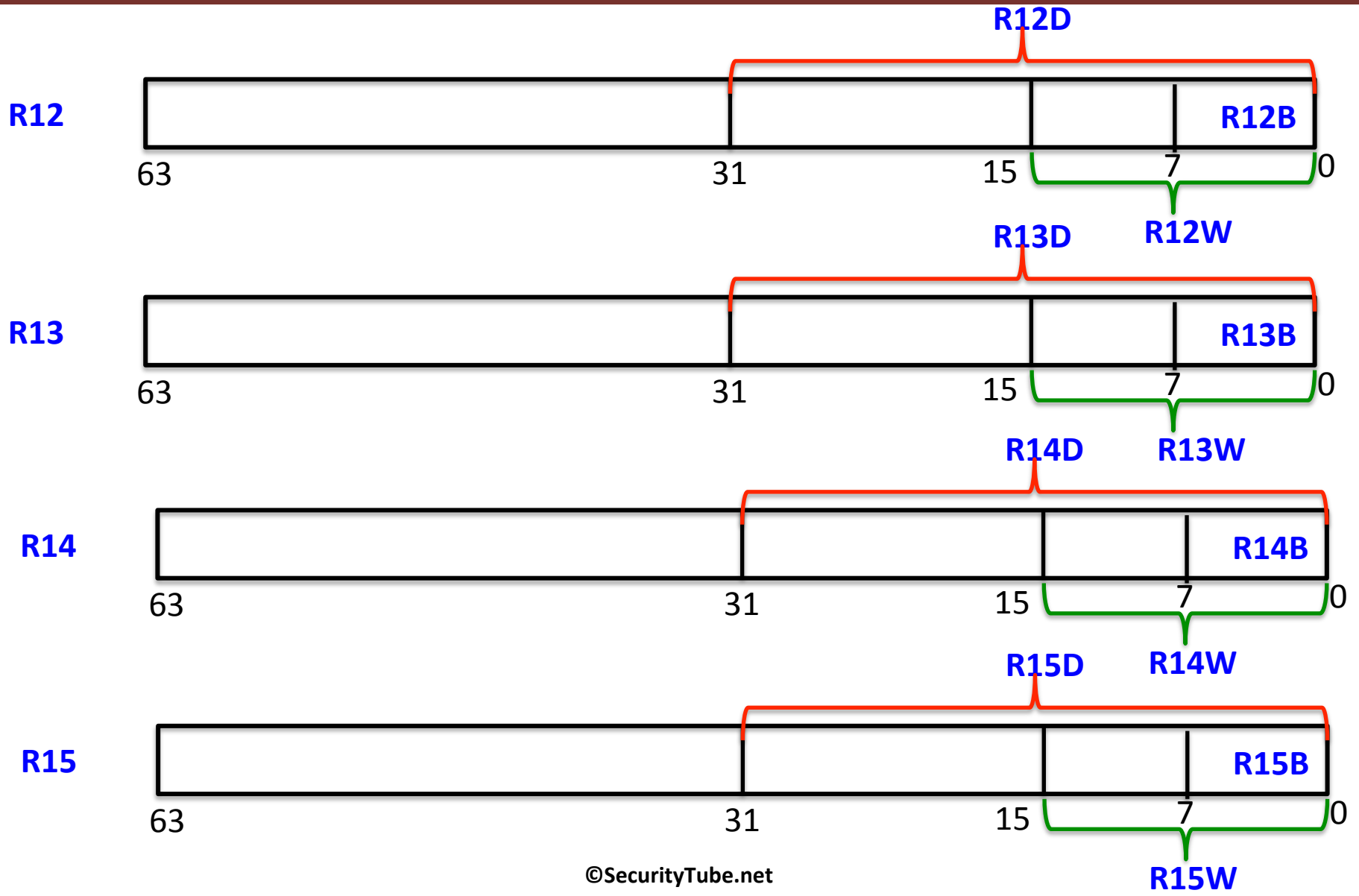
General Purpose Registers



General Purpose Registers



General Purpose Registers



Very Very Important

Table 3-2. Addressable General Purpose Registers

Register Type	Without REX	With REX
Byte Registers	AL, BL, CL, DL, AH, BH, CH, DH	AL, BL, CL, DL, DIL, SIL, BPL, SPL, R8L - R15L
Word Registers	AX, BX, CX, DX, DI, SI, BP, SP	AX, BX, CX, DX, DI, SI, BP, SP, R8W - R15W
Doubleword Registers	EAX, EBX, ECX, EDX, EDI, ESI, EBP, ESP	EAX, EBX, ECX, EDX, EDI, ESI, EBP, ESP, R8D - R15D
Quadword Registers	N.A.	RAX, RBX, RCX, RDX, RDI, RSI, RBP, RSP, R8 - R15

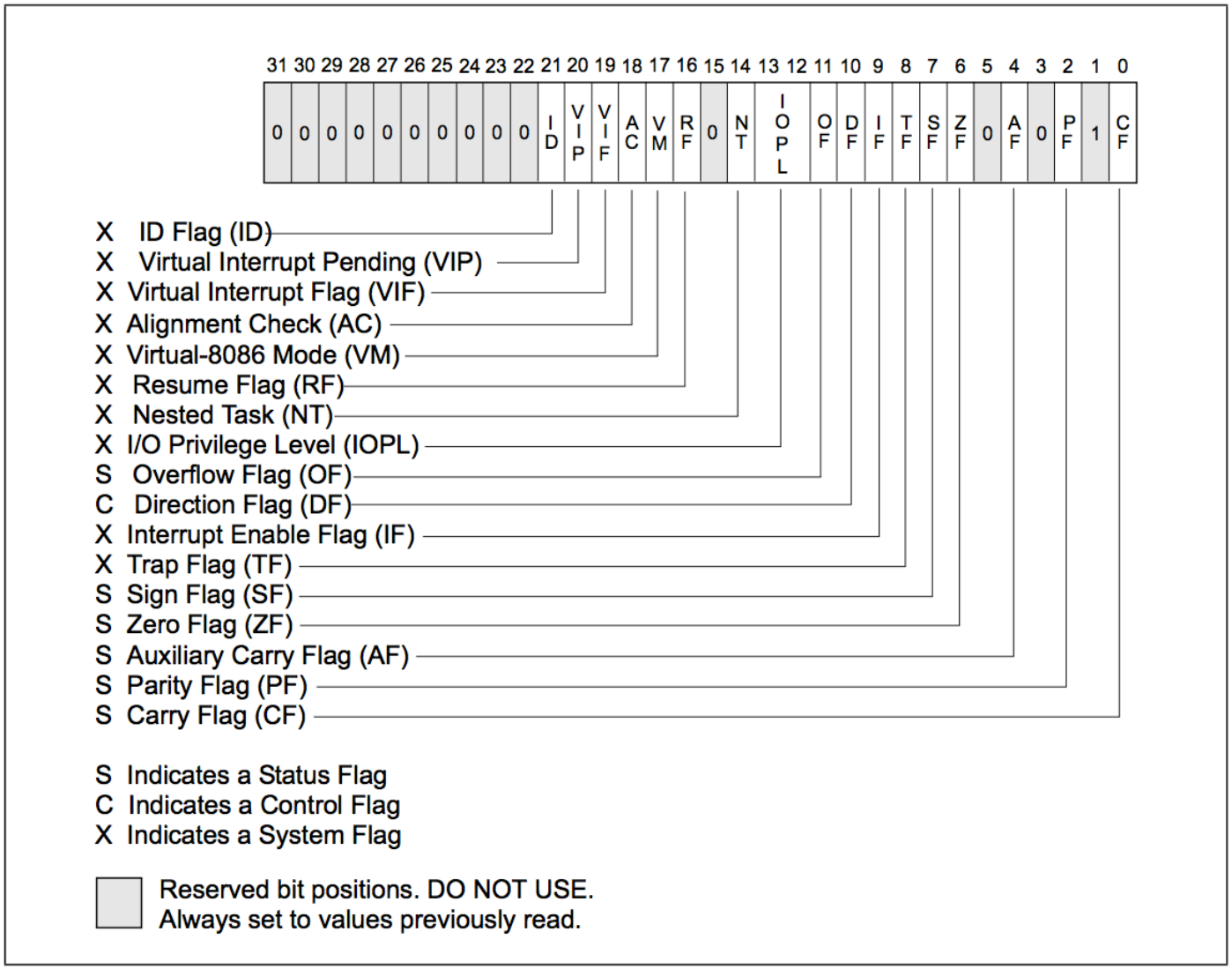
In 64-bit mode, there are limitations on accessing byte registers. An instruction cannot reference legacy high-bytes (for example: AH, BH, CH, DH) and one of the new byte registers at the same time (for example: the low byte of the RAX register). However, instructions may reference legacy low-bytes (for example: AL, BL, CL or DL) and new byte registers at the same time (for example: the low byte of the R8 register, or RBP). The architecture enforces this limitation by changing high-byte references (AH, BH, CH, DH) to low byte references (BPL, SPL, DIL, SIL: the low 8 bits for RBP, RSP, RDI and RSI) for instructions using a REX prefix.

When in 64-bit mode, operand size determines the number of valid bits in the destination general-purpose register:

- 64-bit operands generate a 64-bit result in the destination general-purpose register.
- 32-bit operands generate a 32-bit result, zero-extended to a 64-bit result in the destination general-purpose register.
- 8-bit and 16-bit operands generate an 8-bit or 16-bit result. The upper 56 bits or 48 bits (respectively) of the destination general-purpose register are not modified by the operation. If the result of an 8-bit or 16-bit operation is intended for 64-bit address calculation, explicitly sign-extend the register to the full 64-bits.

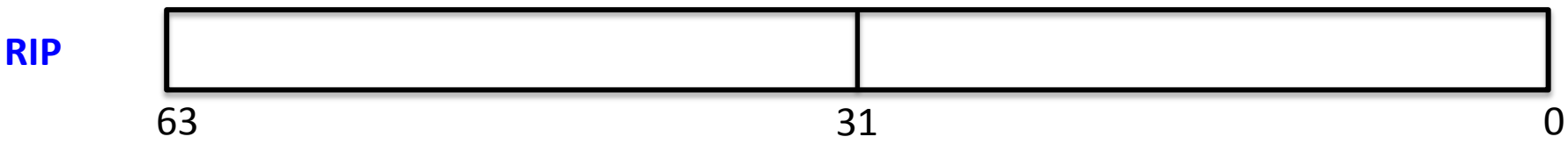
Source: Intel Manual

RFLAGS = Reserved 32-bits + EFLAGS Register



Ref: Intel manual for IA-32

RIP



- Instruction Pointer
- Holy grail for Shellcoding, Exploit Research etc.
- Support RIP Relative Addressing which makes Shellcoding easier

Intel Manuals

- Architecture and Software Development Docs

http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html