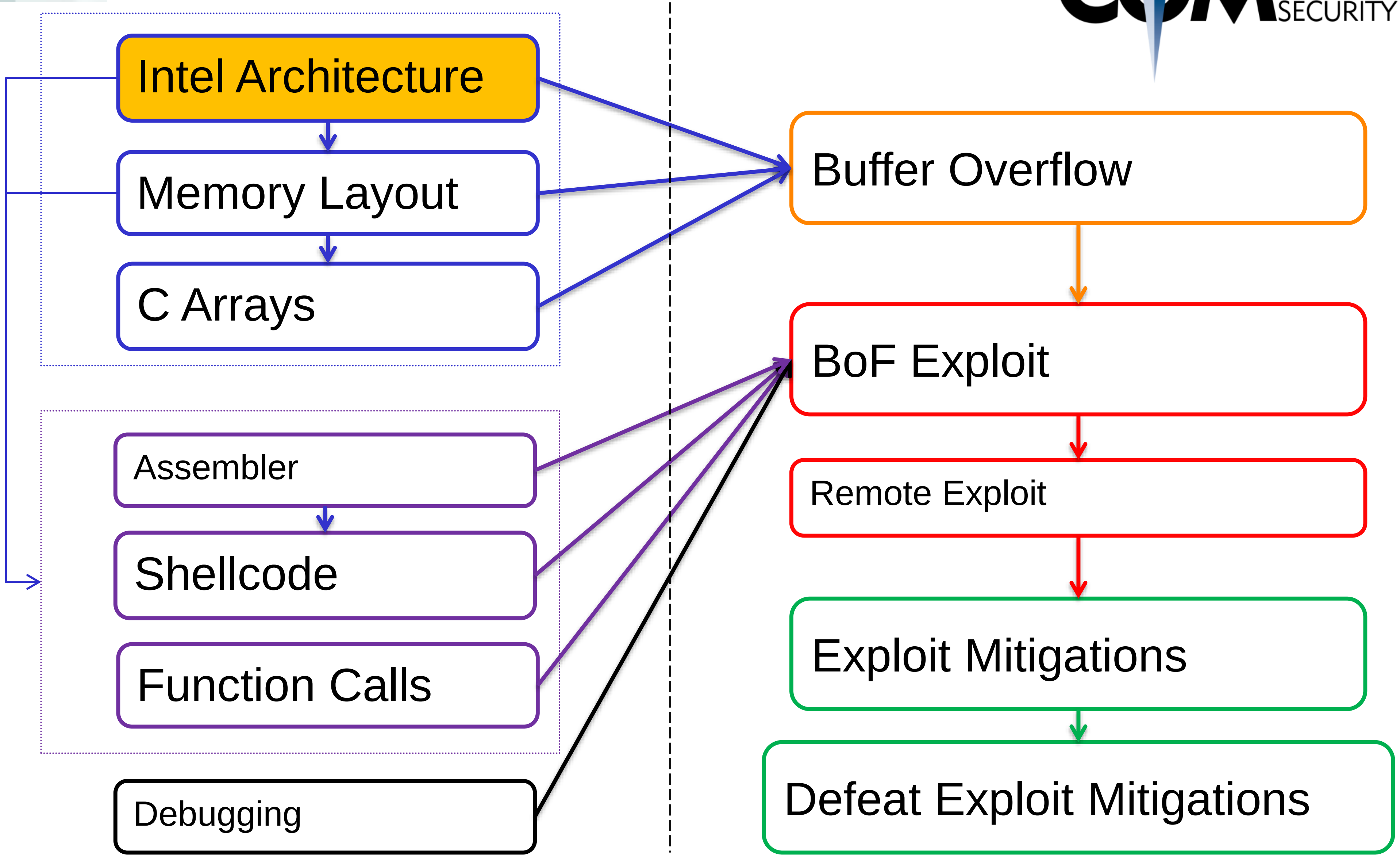
Intel Architecture

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Content



Intel Architecture
Memory Layout
C Arrays
Assembler
Shellcode
Function Calls
Debugging
Buffer Overflow
BoF Exploit
Remote Exploit
Exploit Mitigations
Defeat Exploit Mitigations

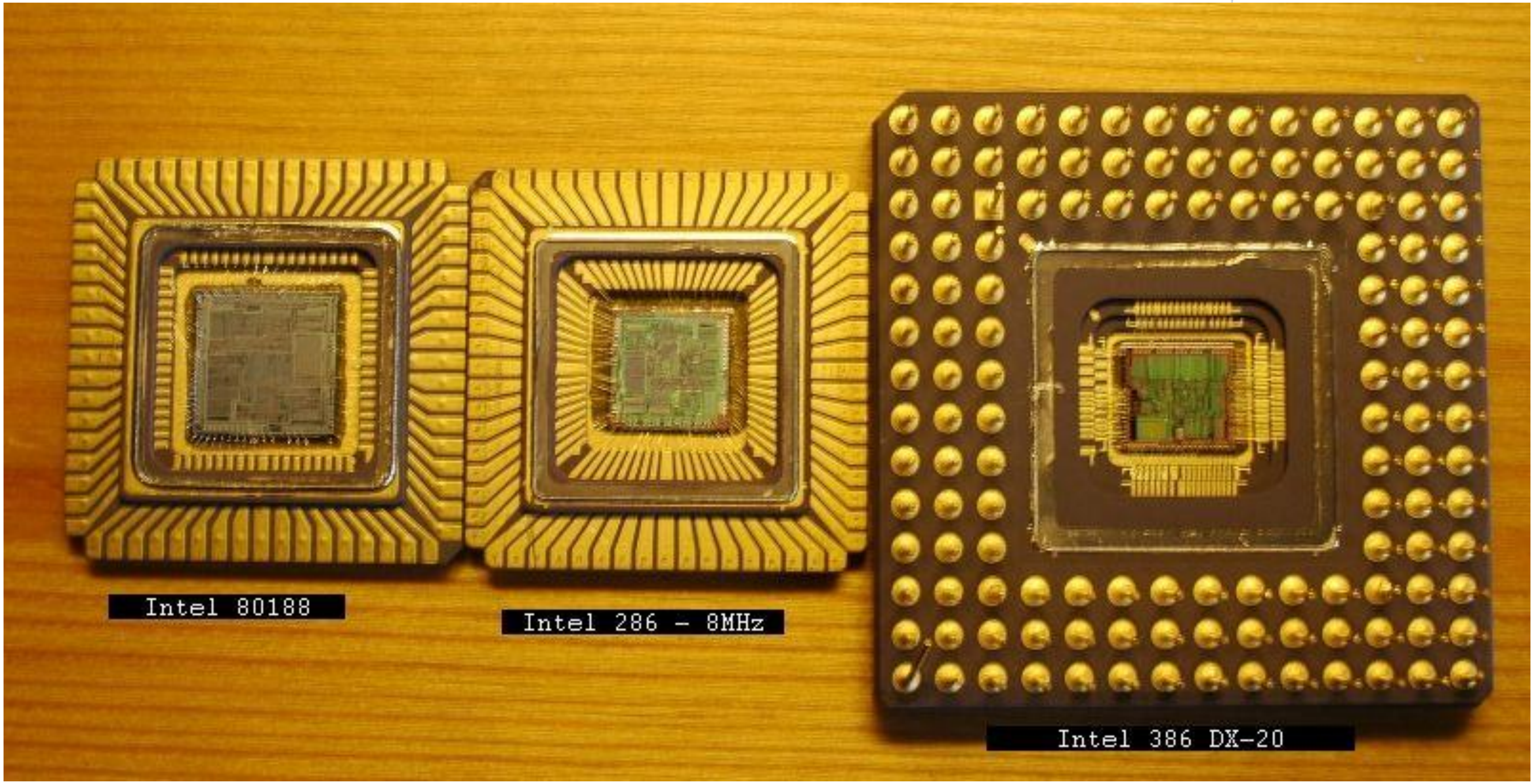
Intel Architecture
Intel CPU

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Intel CPU

Intel CPU

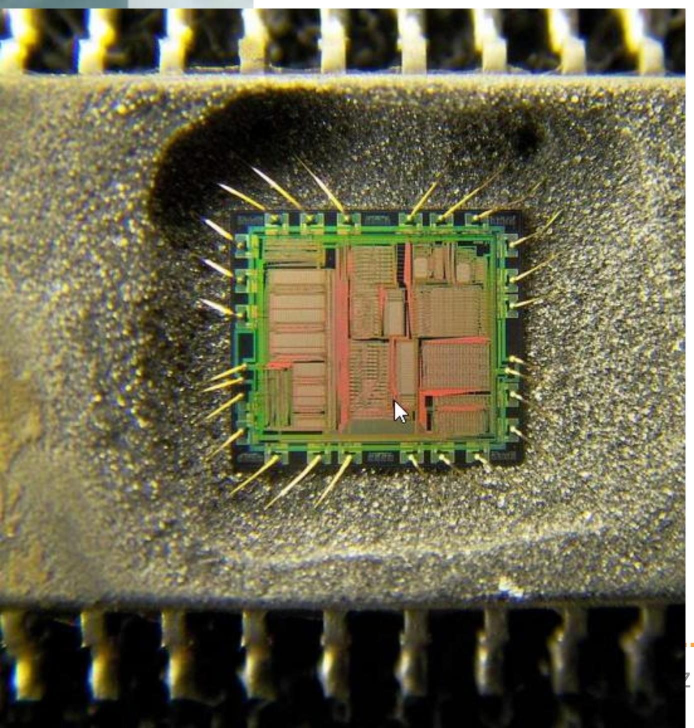


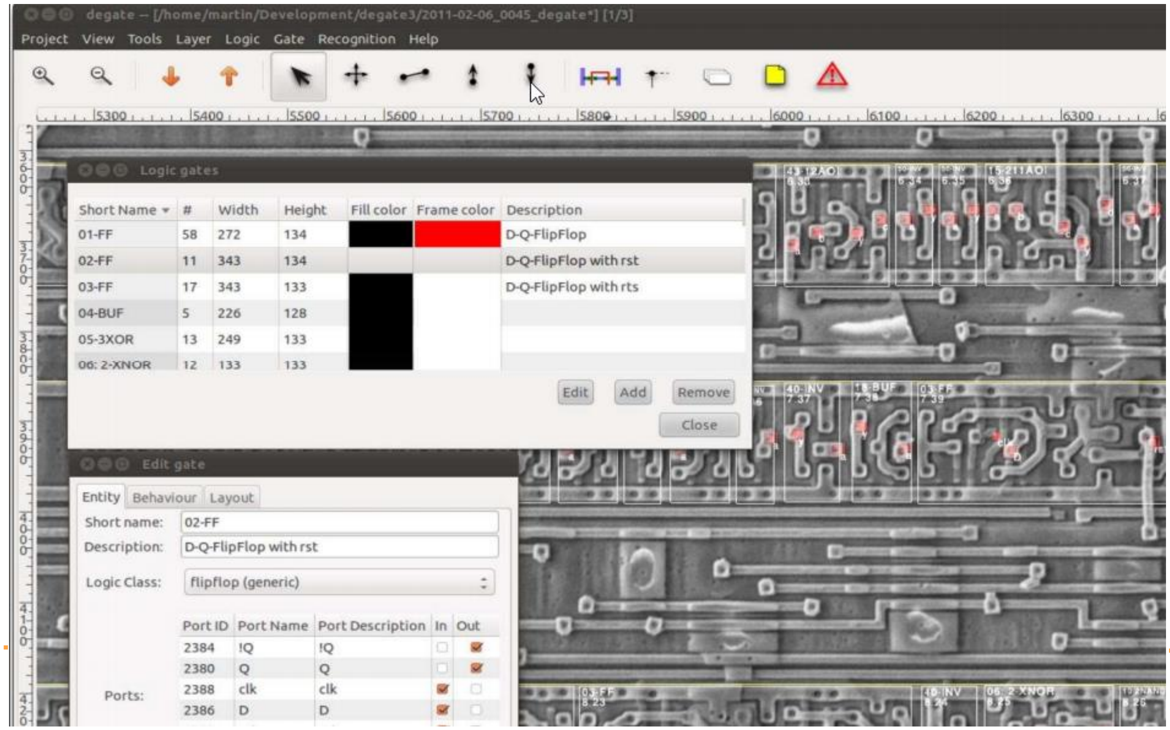
Intermezzo: Chip De-caping and Analysis

http://www.bluehatil.com/files/Extracting%20Secrets%20from%20Silicon%20%E2%80%93%20A%20New%20Generation%20of%20Bug%20Hunting.pdf

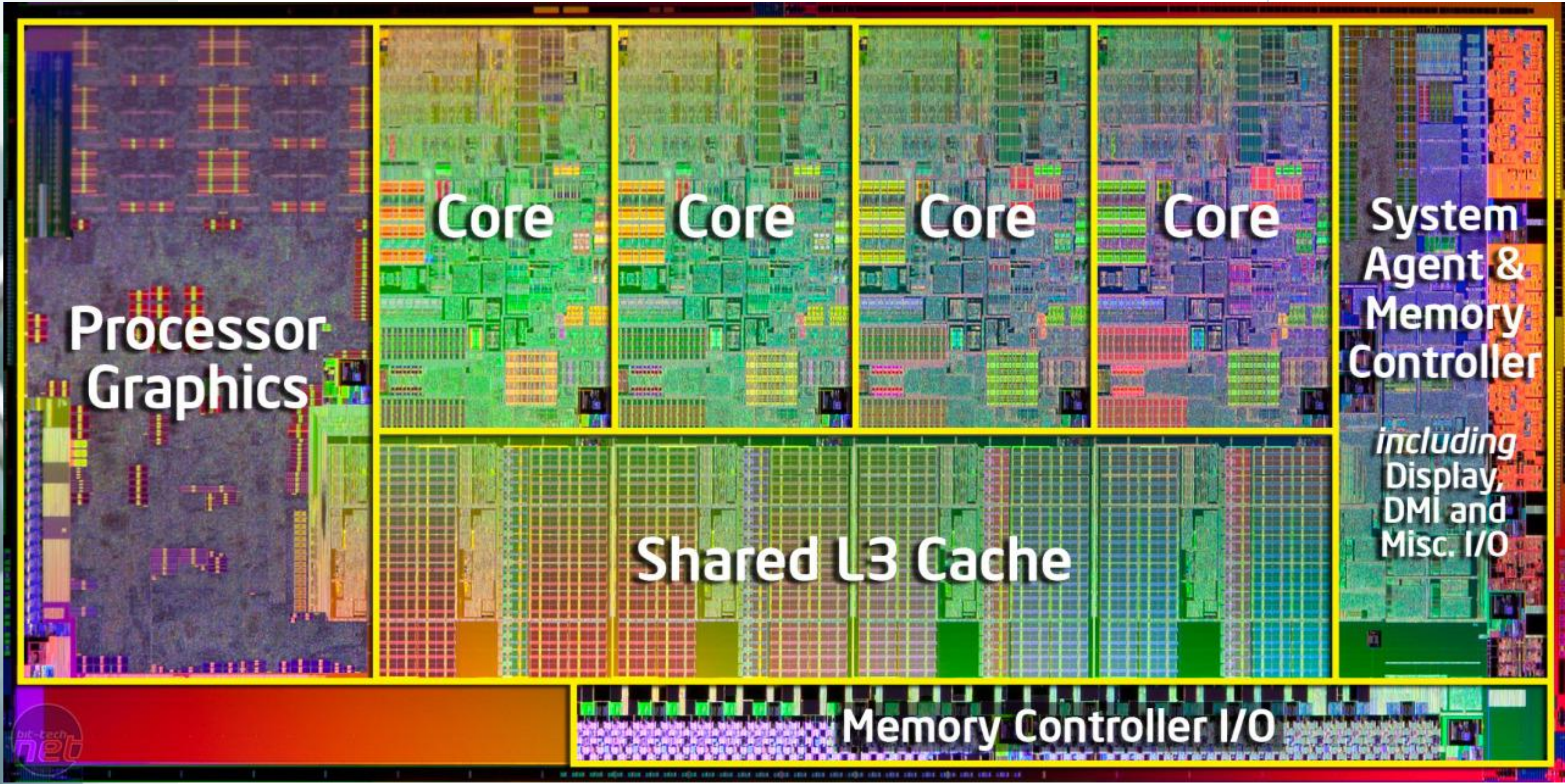
Extracting Secrets from Silicon – A New Generation of Bug Hunting

- Gunter Ollmann, Microsoft
- Blue Hat Security



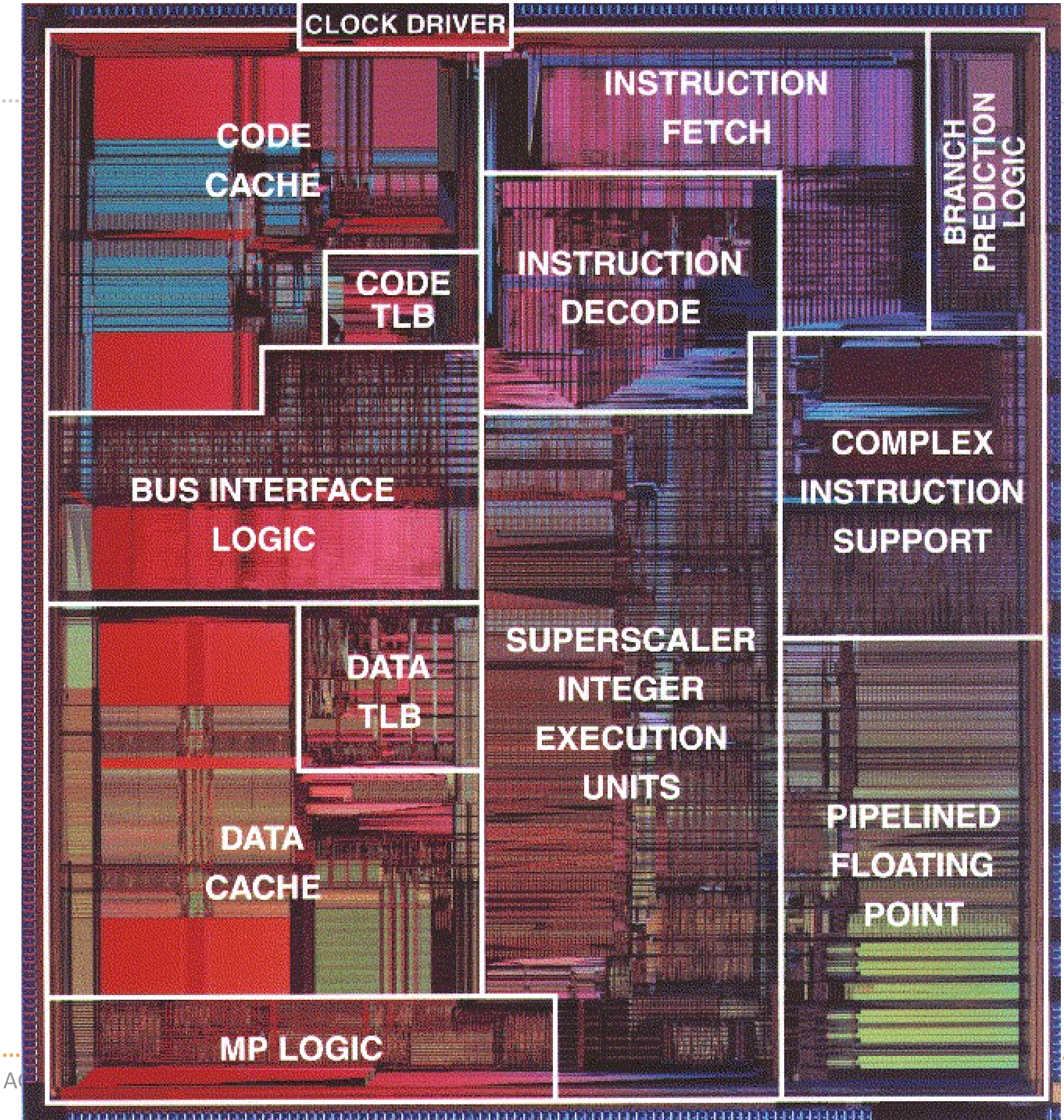


Intel CPU

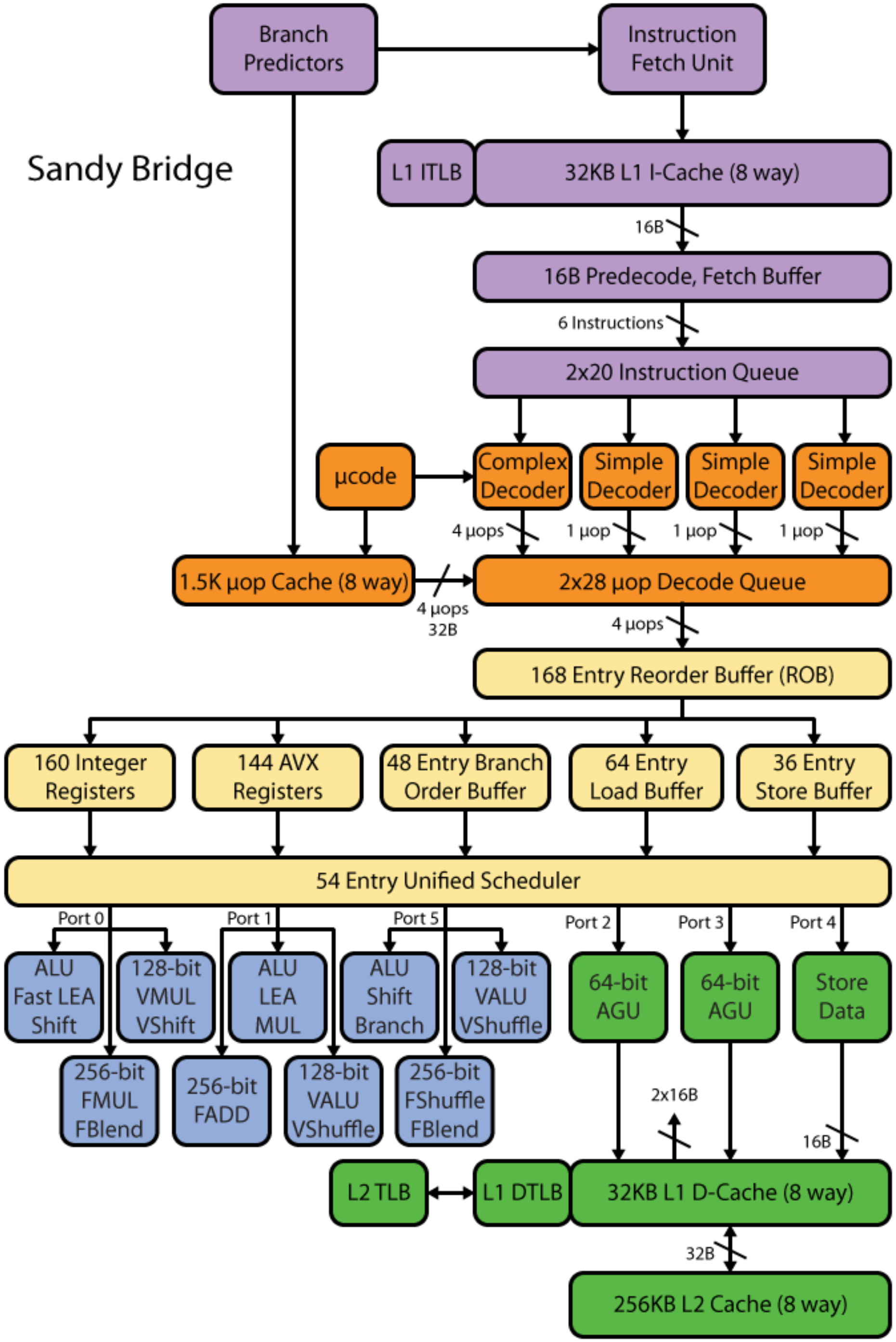

Processor Graphics
Core
Core
Core
Core
System Agent & Memory Controller
including Display, DMI and Misc. I/O
Shared L3 Cache
Memory Controller I/O

Intel CPU

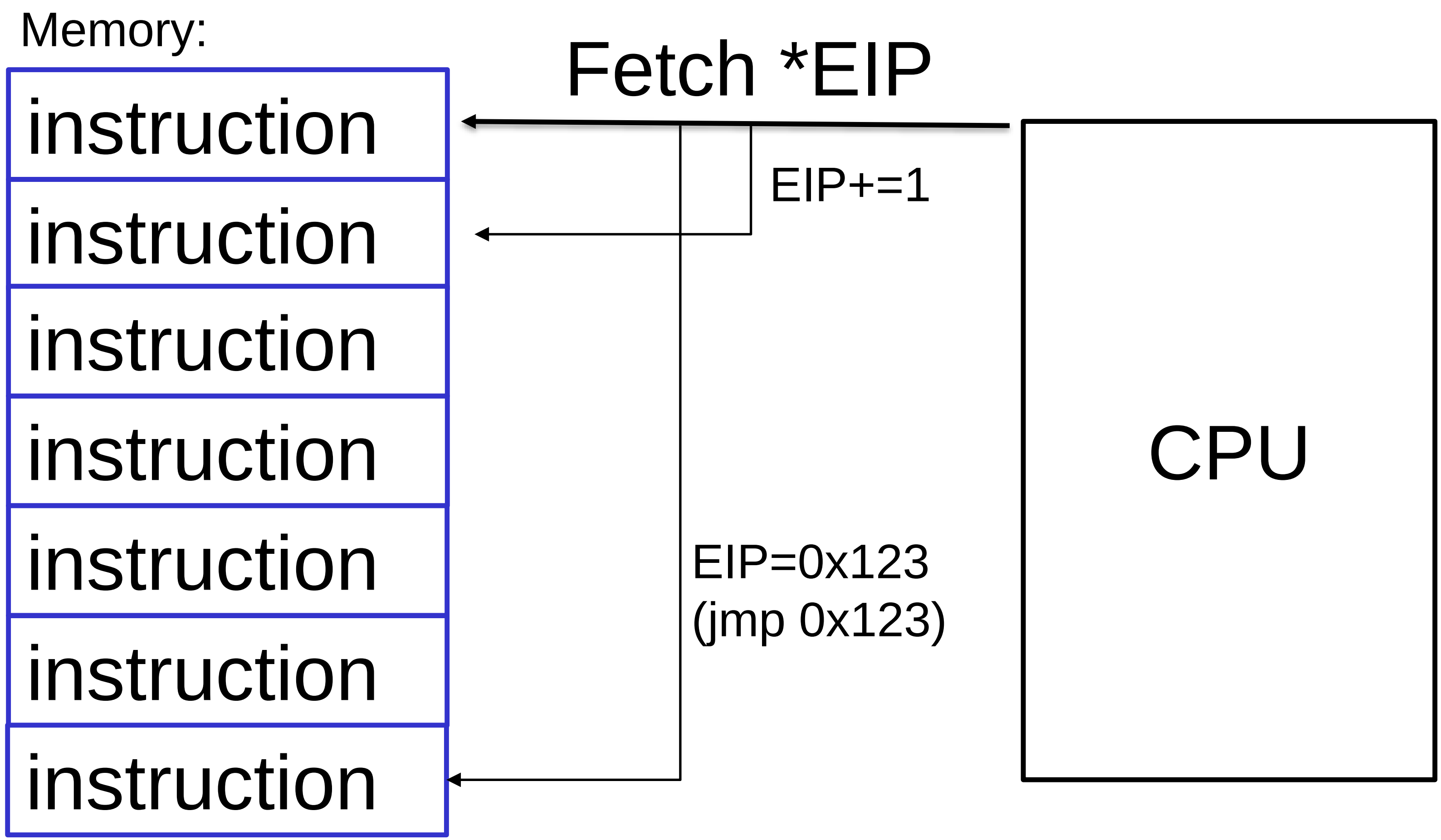
Pentium Die



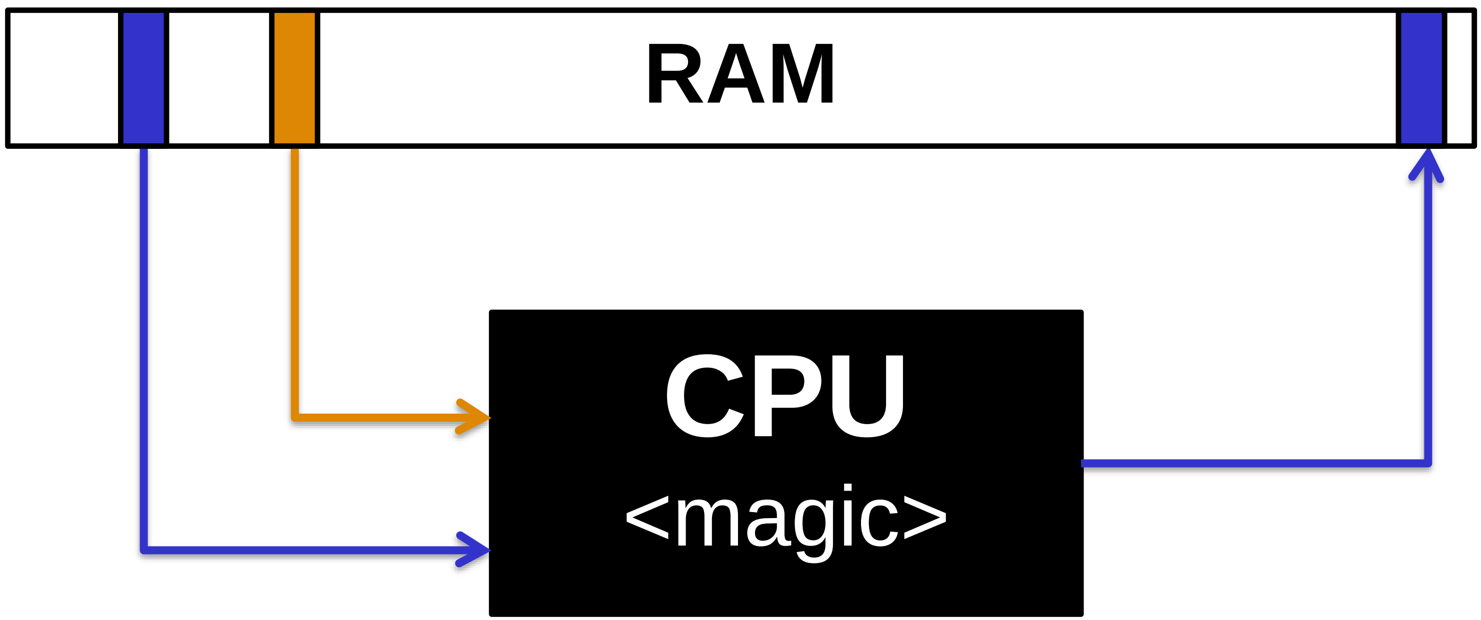
Sandy Bridge



Overview: Computerz



Overview: Computerz



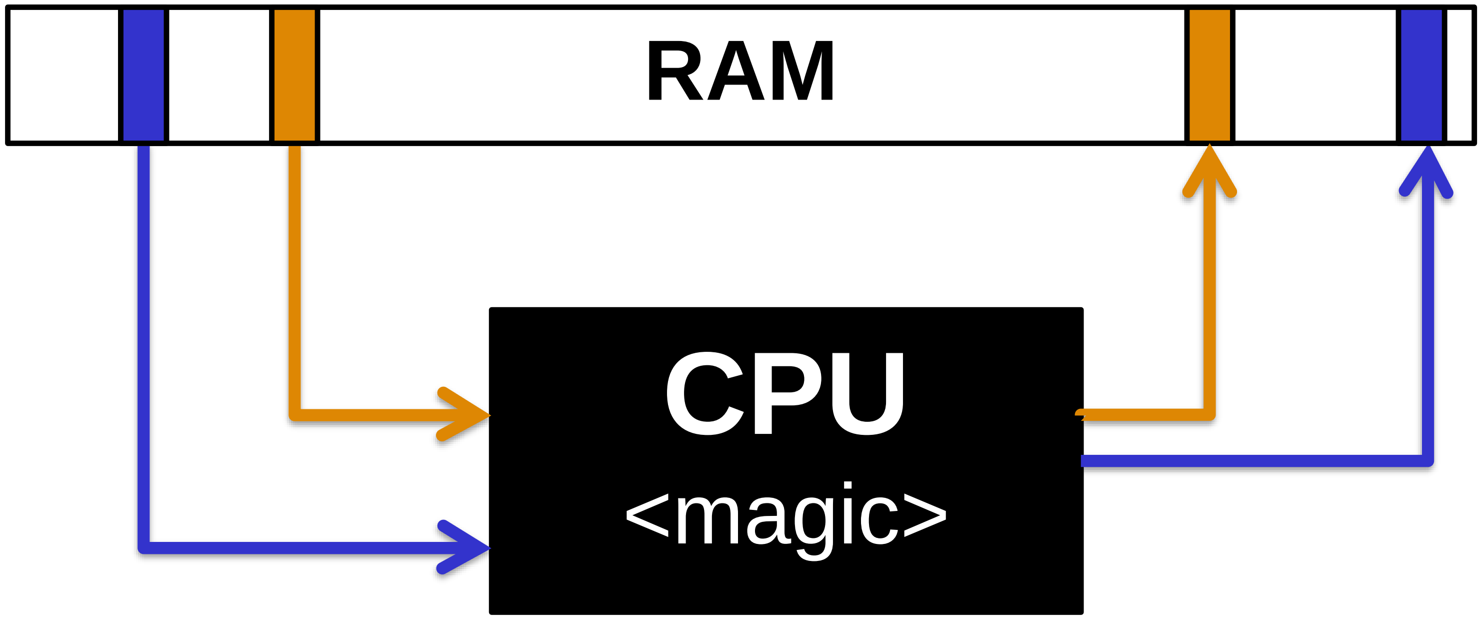
Read:

- Data
- Instructions

Write:

- Data

von Neumann Architecture



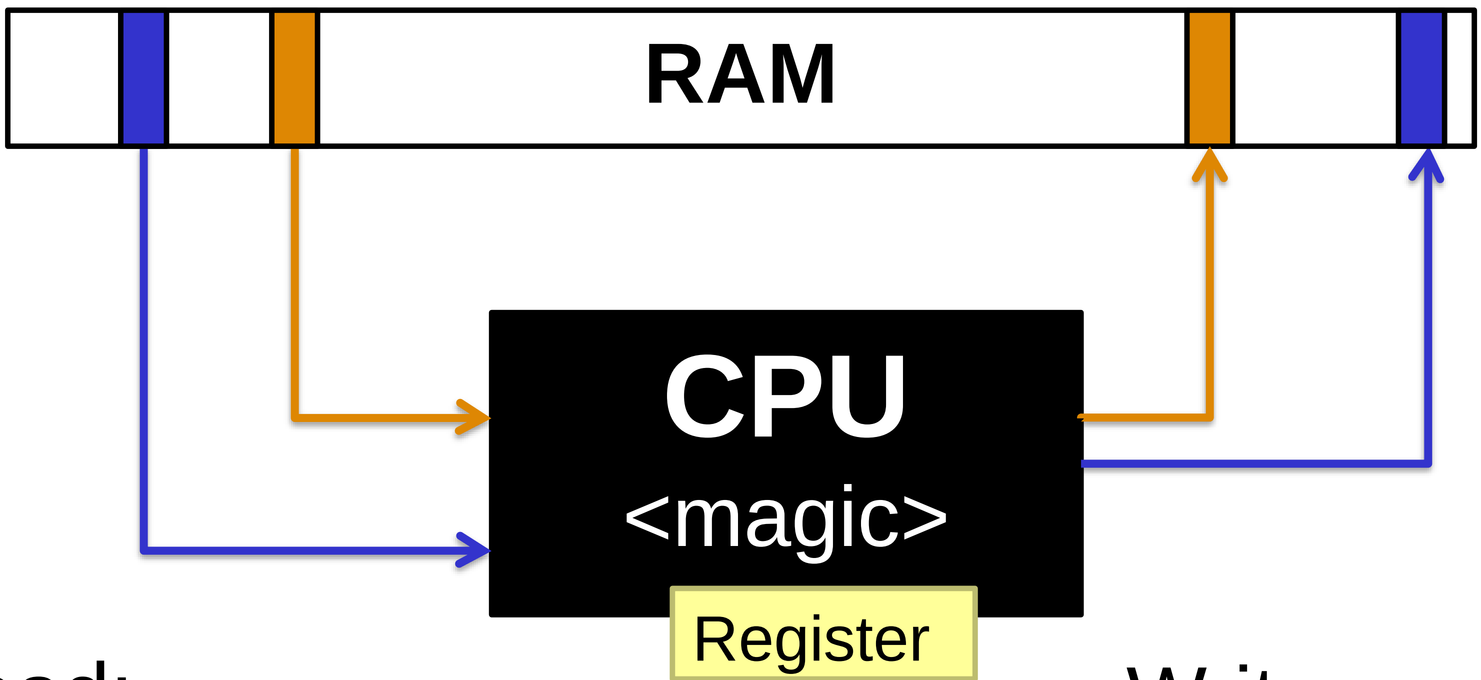
Read:

- Data
- Instructions

Write:

- Data
- Instructions

Overview: Computerz



Read:

- Data
- Instructions

Write:

- Data
- Instructions

Register are the “variables” on the CPU

Immediate access for the CPU

Cannot write Memory -> Memory

- Always: Memory -> Register -> Memory

Register: <1 cycle
L1: ~3
L2: ~14
RAM: ~240

Overview: CPU Registers

Register can hold:

- Data (numbers)
- Addresses (also numbers, but with a different meaning)

Registers can be used to:

- Perform computations
- Read / Write memory
- Execute instructions

Overview: CPU Registers

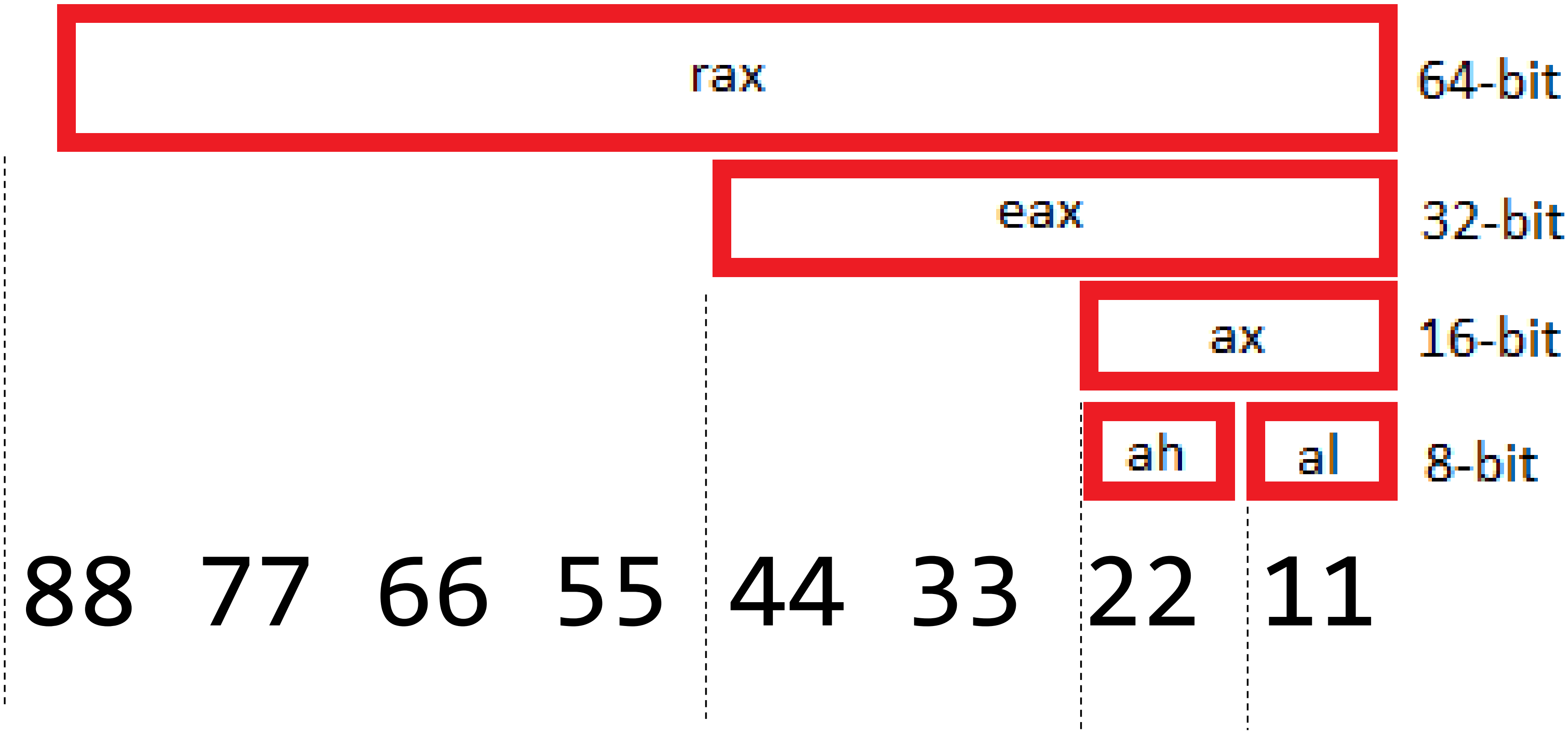
32	64	Acronym	
EAX	RAX	Accumulator	Adding stuff
EBX	RBX	Base	Referencing stuff
ECX	RCX	Count	Counting stuff
EDX	RDX	Data	Stuff
ESI	RSI	Source Index	Points to a source
EDI	RDI	Destination Index	Points to a destination
	R8-R15		General Purpose

Overview: CPU Registers

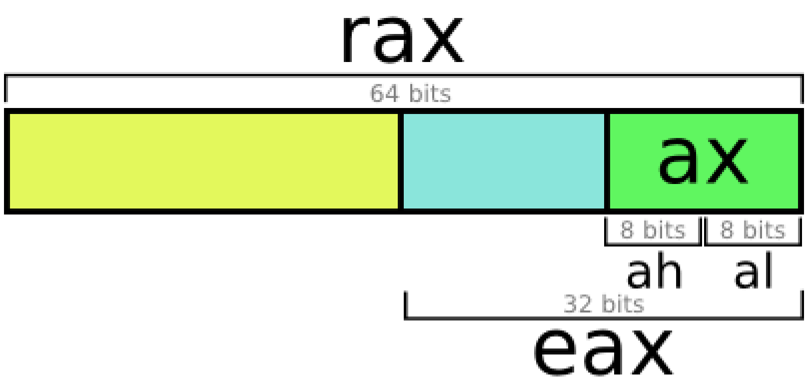
32	64	Acronym	Points to?
EIP	RIP	Instruction Pointer	Next instruction to be executed
ESP	RSP	Stack Pointer	Top of Stack
EBP	RBP	Base Pointer	Current Stack Frame (Bottom)

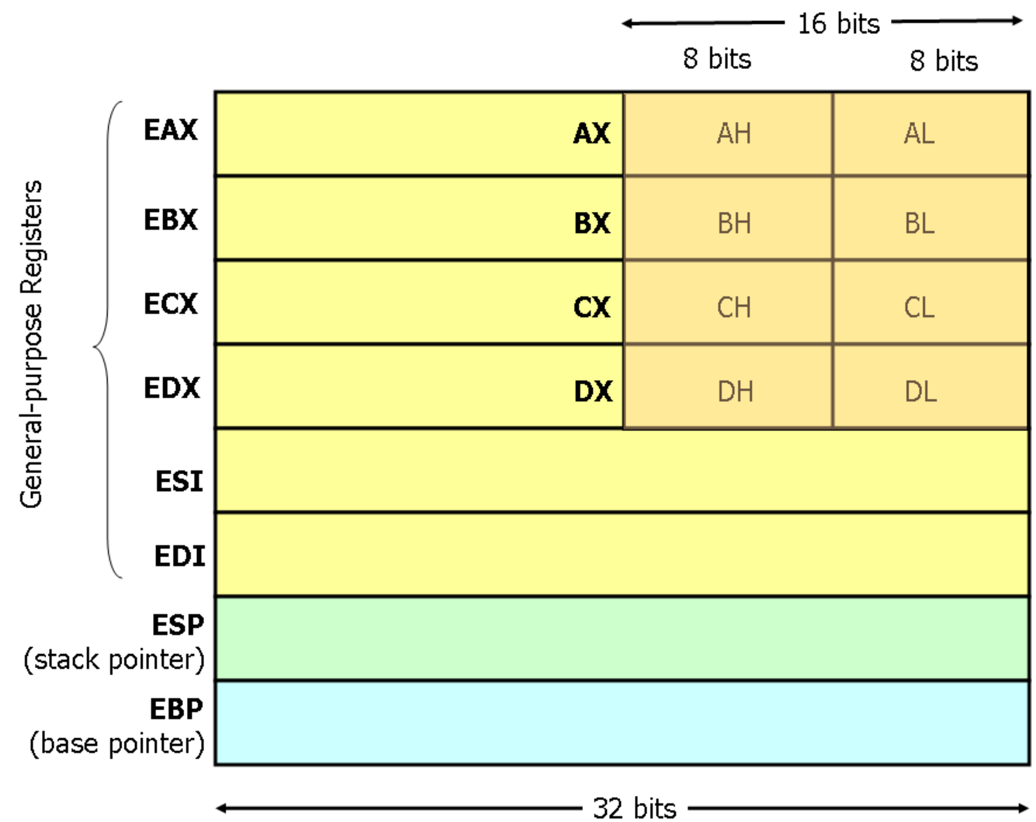
Print this slide and stick it on your bathroom mirror

Overview: CPU Registers



Overview: CPU Registers





Overview: CPU Registers

Fun Fact: Current Intel CPU’s are compatible to the 8086

8086:

- From 1978
- 5-10mhz

Overview: CPU Registers

Recap:

- CPU work with **registers**
- Registers can hold **data**
- Registers can also hold **addresses** of memory locations (to write data to)
- They can be 32 bit (**E**AX) or 64 bit (**R**AX)
- Some registers are multi-purpose
- Some registers are special (RIP, RBP, RSP)

CPU Instructions

CPU in a few instructions:

```
instr = 0x01 0xA0 0xB0

switch instr[0]:
  case 0x01:
       add( instr[1], instr[2] )
  case 0x02:
       sub( instr[1], instr[2] )
…
```

CPU Instructions

Intel x86 Assembler Instruction Set Opcode Table

ADD Eb Gb *00*	**ADD** Ev Gv *01*	**ADD** Gb Eb *02*	**ADD** Gv Ev *03*	**ADD** AL Ib *04*	**ADD** eAX Iv *05*	**PUSH** ES *06*	**POP** ES *07*	**OR** Eb Gb *08*	**OR** Ev Gv *09*	**OR** Gb Eb *0A*	**OR** Gv Ev *0B*	**OR** AL Ib *0C*	**OR** eAX Iv *0D*	**PUSH** CS *0E*	**TWOBYTE** *0F*
ADC Eb Gb *10*	**ADC** Ev Gv *11*	**ADC** Gb Eb *12*	**ADC** Gv Ev *13*	**ADC** AL Ib *14*	**ADC** eAX Iv *15*	**PUSH** SS *16*	**POP** SS *17*	**SBB** Eb Gb *18*	**SBB** Ev Gv *19*	**SBB** Gb Eb *1A*	**SBB** Gv Ev *1B*	**SBB** AL Ib *1C*	**SBB** eAX Iv *1D*	**PUSH** DS *1E*	**POP** DS *1F*
AND Eb Gb *20*	**AND** Ev Gv *21*	**AND** Gb Eb *22*	**AND** Gv Ev *23*	**AND** AL Ib *24*	**AND** eAX Iv *25*	**ES:** *26*	**DAA** *27*	**SUB** Eb Gb *28*	**SUB** Ev Gv *29*	**SUB** Gb Eb *2A*	**SUB** Gv Ev *2B*	**SUB** AL Ib *2C*	**SUB** eAX Iv *2D*	**CS:** *2E*	**DAS** *2F*
XOR Eb Gb *30*	**XOR** Ev Gv *31*	**XOR** Gb Eb *32*	**XOR** Gv Ev *33*	**XOR** AL Ib *34*	**XOR** eAX Iv *35*	**SS:** *36*	**AAA** *37*	**CMP** Eb Gb *38*	**CMP** Ev Gv *39*	**CMP** Gb Eb *3A*	**CMP** Gv Ev *3B*	**CMP** AL Ib *3C*	**CMP** eAX Iv *3D*	**DS:** *3E*	**AAS** *3F*
INC eAX *40*	**INC** eCX *41*	**INC** eDX *42*	**INC** eBX *43*	**INC** eSP *44*	**INC** eBP *45*	**INC** eSI *46*	**INC** eDI *47*	**DEC** eAX *48*	**DEC** eCX *49*	**DEC** eDX *4A*	**DEC** eBX *4B*	**DEC** eSP *4C*	**DEC** eBP *4D*	**DEC** eSI *4E*	**DEC** eDI *4F*
PUSH eAX *50*	**PUSH** eCX *51*	**PUSH** eDX *52*	**PUSH** eBX *53*	**PUSH** eSP *54*	**PUSH** eBP *55*	**PUSH** eSI *56*	**PUSH** eDI *57*	**POP** eAX *58*	**POP** eCX *59*	**POP** eDX *5A*	**POP** eBX *5B*	**POP** eSP *5C*	**POP** eBP *5D*	**POP** eSI *5E*	**POP** eDI *5F*
PUSHA *60*	**POPA** *61*	**BOUND** Gv Ma *62*	**ARPL** Ew Gw *63*	**FS:** *64*	**GS:** *65*	**OPSIZE:** *66*	**ADSIZE:** *67*	**PUSH** Iv *68*	**IMUL** Gv Ev Iv *69*	**PUSH** Ib *6A*	**IMUL** Gv Ev Ib *6B*	**INSB** Yb DX *6C*	**INSW** Yz DX *6D*	**OUTSB** DX Xb *6E*	**OUTSW** DX Xv *6F*
JO Jb *70*	**JNO** Jb *71*	**JB** Jb *72*	**JNB** Jb *73*	**JZ** Jb *74*	**JNZ** Jb *75*	**JBE** Jb *76*	**JA** Jb *77*	**JS** Jb *78*	**JNS** Jb *79*	**JP** Jb *7A*	**JNP** Jb *7B*	**JL** Jb *7C*	**JNL** Jb *7D*	**JLE** Jb *7E*	**JNLE** Jb *7F*
ADD Eb Ib *80*	**ADD** Ev Iv *81*	**SUB** Eb Ib *82*	**SUB** Ev Ib *83*	**TEST** Eb Gb *84*	**TEST** Ev Gv *85*	**XCHG** Eb Gb *86*	**XCHG** Ev Gv *87*	**MOV** Eb Gb *88*	**MOV** Ev Gv *89*	**MOV** Gb Eb *8A*	**MOV** Gv Ev *8B*	**MOV** Ew Sw *8C*	**LEA** Gv M *8D*	**MOV** Sw Ew *8E*	**POP** Ev *8F*

Add

Opcode	Mnemonic	Description
04 ib	ADD AL, imm8	Add imm8 to AL
05 iw	ADD AX, imm16	Add imm16 to AX
05 id	ADD EAX, imm32	Add imm32 to EAX
80 /0 ib	ADD r/m8, imm8	Add imm8 to r/m8
81 /0 iw	ADD r/m16, imm16	Add imm16 to r/m16
81 /0 id	ADD r/m32, imm32	Add imm32 to r/m32
83 /0 ib	ADD r/m16, imm8	Add sign-extended imm8 to r/m16
83 /0 ib	ADD r/m32, imm8	Add sign-extended imm8 to r/m32
00 /r	ADD r/m8, r8	Add r8 to r/m8
01 /r	ADD r/m16, r16	Add r16 to r/m16
01 /r	ADD r/m32, r32	Add r32 to r/m32
02 /r	ADD r8, r/m8	Add r/m8 to r8
03 /r	ADD r16, r/m16	Add r/m16 to r16
03 /r	ADD r32, r/m32	Add r/m32 to r32

Description

Adds the first operand (destination operand) and the second operand (source operand) and stores the result in the destination operand. The destination operand can be a register or a memory location; the source operand can be an immediate, a register, or a memory location. (However, two memory operands cannot be used in one instruction.) When an immediate value is used as an operand, it is sign-extended to the length of the destination operand format.

The ADD instruction performs integer addition. It evaluates the result for both signed and unsigned integer operands and sets the OF and CF flags to indicate a carry (overflow) in the signed or unsigned result, respectively. The SF flag indicates the sign of the signed result.

This instruction can be used with a LOCK prefix to allow the instruction to be executed atomically.

Operation

```
Destination = Destination + Source;
```

CPU Instructions

```
83 c4 08                add     $0x8,%rsp
83 c3 01                add     $0x1,%rbx
83 44 24 0c 01          addl    $0x1,0xc(%rsp)
83 05 41 94 2c 00 01    addl    $0x1,0x2c9441(%rip)
```

CPU Instructions

Recap:

- CPU looks at bytes, and then decides what to execute based on them

Hex Numbers, and Little Endian

A guide to understand the rest of my slides

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Hex Numbers, and Little Endian

Intel CPU's

- 1 Byte = 8 Bit
- Little endian

Hex Numbers, and Little Endian

Intel CPU's

- 1 Byte = 8 Bit
- Little endian

Others:

- CDC 6000: 18, 24 and 60 bit
- PDP1/9/15: 18 bit words
- Apollo Guidance Computer: 15 bit

- ARM and other RISC: Big Endian

Decimal Numbers

Decimal: 0 1 2 3 4 5 6 7 8 9

1 decimal digit: 10 values

2 hex digits: 100 values

10 * 10 = 100

Hex Numbers

Hex: 0 1 2 3 4 5 6 7 8 9 A B C D E F

1 hex digit: 16 values (4 bit, 2^4)

2 hex digits: 256 values (8 bit, 2^8)

16 * 16 = 256

1 Byte = 8 Bit = 256 values!

Hex numbers

0x00 = 0

0x01 = 1

0x0f = 15

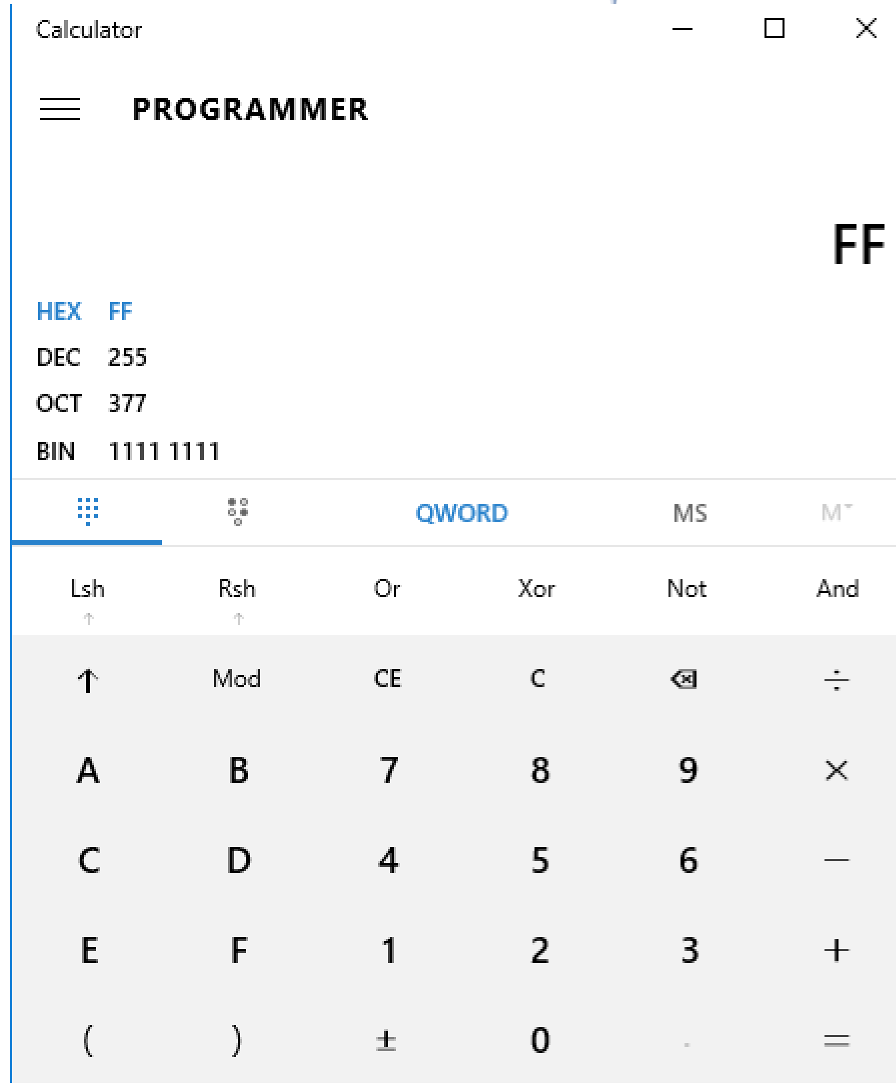
0x10 = 16

0x11 = 17

0x20 = 32

0xf0 = 240

0xff = 255



Hex Numbers

Base 10	**6975**
Base 16	**0x1B3F**
Nibbles	**0001 1011 0011 1111**

Hex Numbers

Base 10	6975
Base 16	0x1B3F
Nibbles	0001 1011 0011 1111
Bytes	0x1B 0x3F

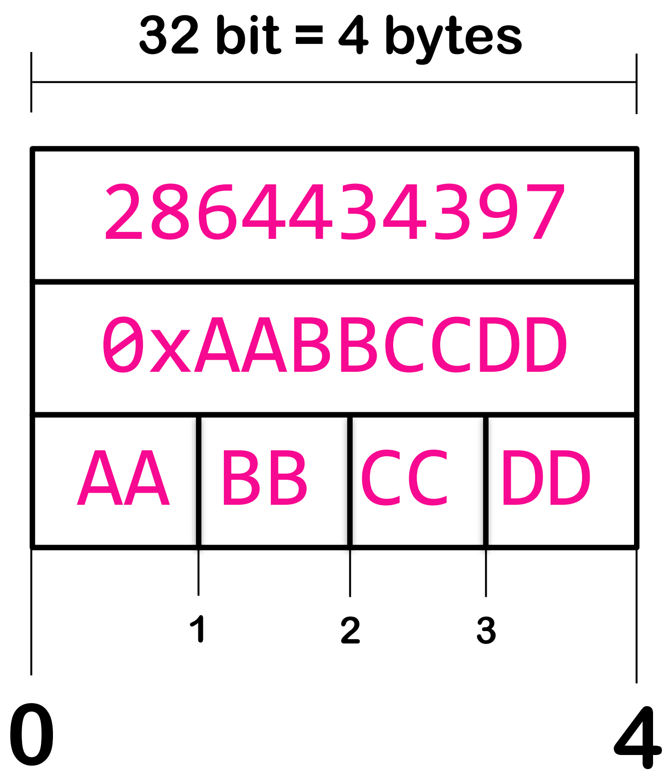
Endianness

Number: 0x1B3F

Big Endian: 0x1B 0x3F 0x1B3F

Little Endian: 0x3F 0x1B 0x3F1B

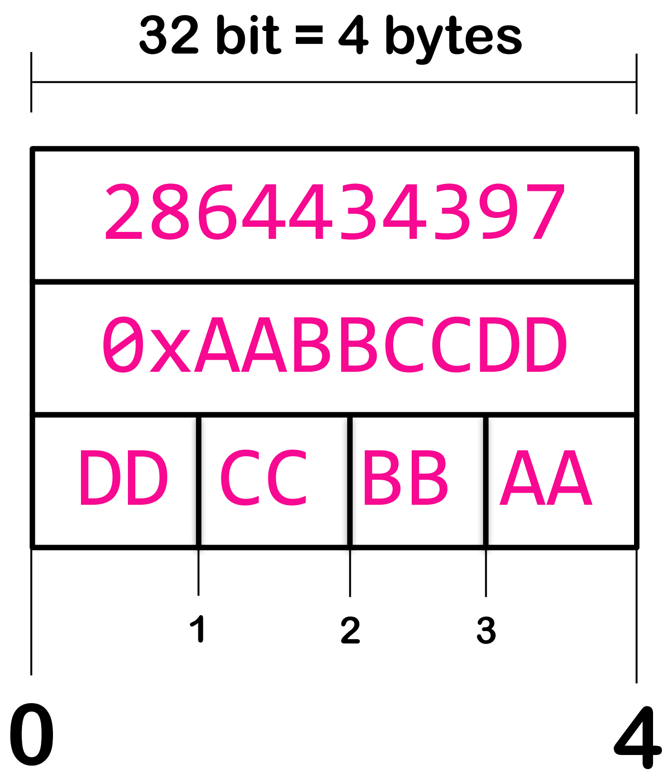
```
f0 32 7d 60 95 48 d0 62  08 80 4b 67 b4 4a 21 dc
80 3f 6c dd 4a f5 a3 d4  ce 32 8d e4 21 d7 a5 5a
92 93 4b f1 ca 0a ce 3c  b9 14 20 a5 00 a4 4a 3e
bd 4b 8c b4 d1 90 2b 25  a9 c8 f4 c8 10 85 fb d6
fc 2a 1f c6 8a 7f 25 e7  47 f4 95 01 e2 d7 82 fe
22 95 fa 8e 49 e4 50 98  d3 84 95 a7 97 1d 97 92
25 32 9f 90 0c a9 07 73  c2 2b 49 06 4c 1a 26 69
b2 75 3e 20 db 65 bf 22  68 cf 29 1b 8a 65 8d 54
91 ba 33 f3 05 59 07 39  cd 43 96 6f 5d 88 bb 7a
```



Number in Decimal (10)

Number in Hex (16)

Big Endian Storage



Number in Decimal (10)

Number in Hex (16)

Little Endian Storage

Endianness: Little Endian (Intel)

DD	CC	BB	AA

Four 8 bit numbers:

- DD
- CC
- BB
- AA

Two 16 bit numbers:

- 0xCCDD
- 0xAABB

A 32 bit number:

- 0xAABBCCDD

??

Number:

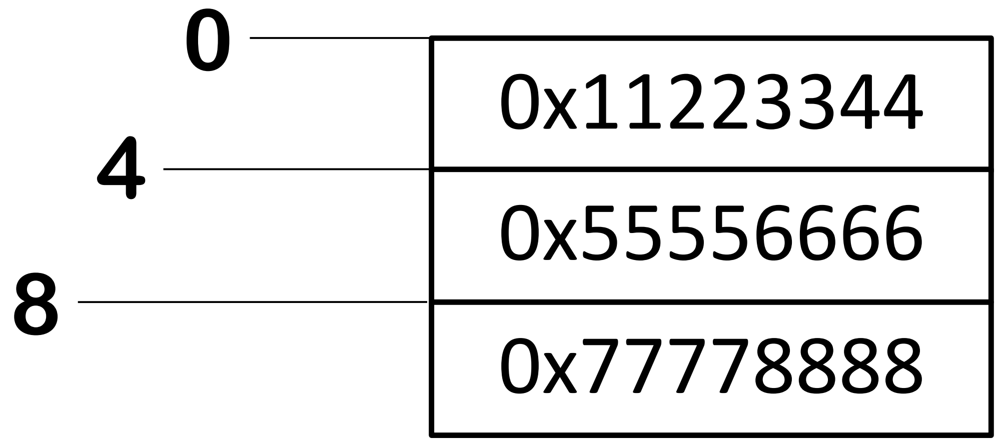
`0x1122334455667788`

Little Endian:

88	77	66	55	44	33	22	11
0	1	2	3	4	5	6	7

Numbers in memory

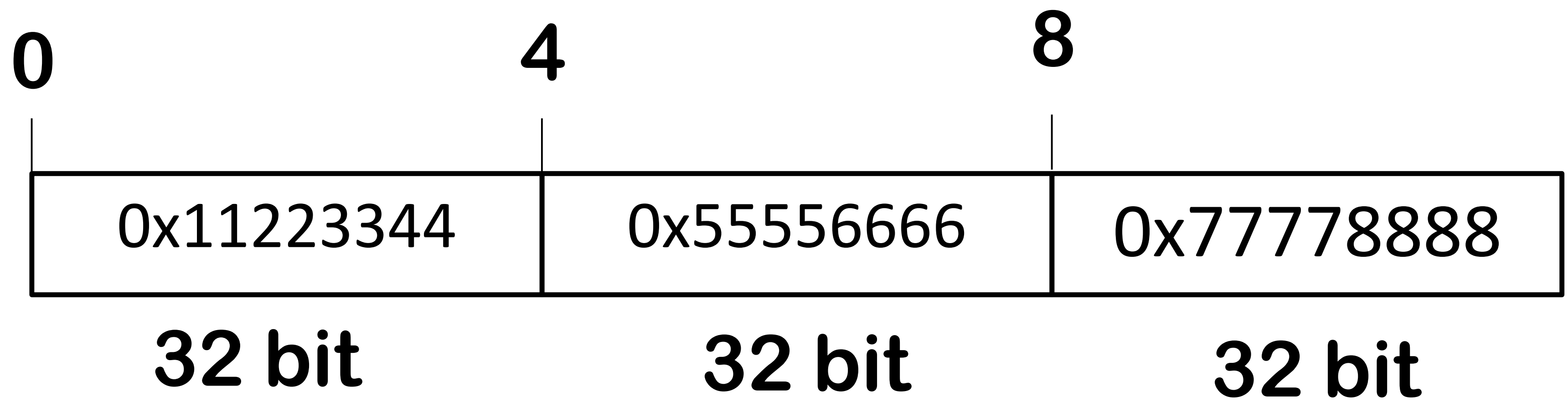
0	0x11223344	32 bit = 4 bytes
4	0x55556666	32 bit = 4 bytes
8	0x77778888	32 bit = 4 bytes



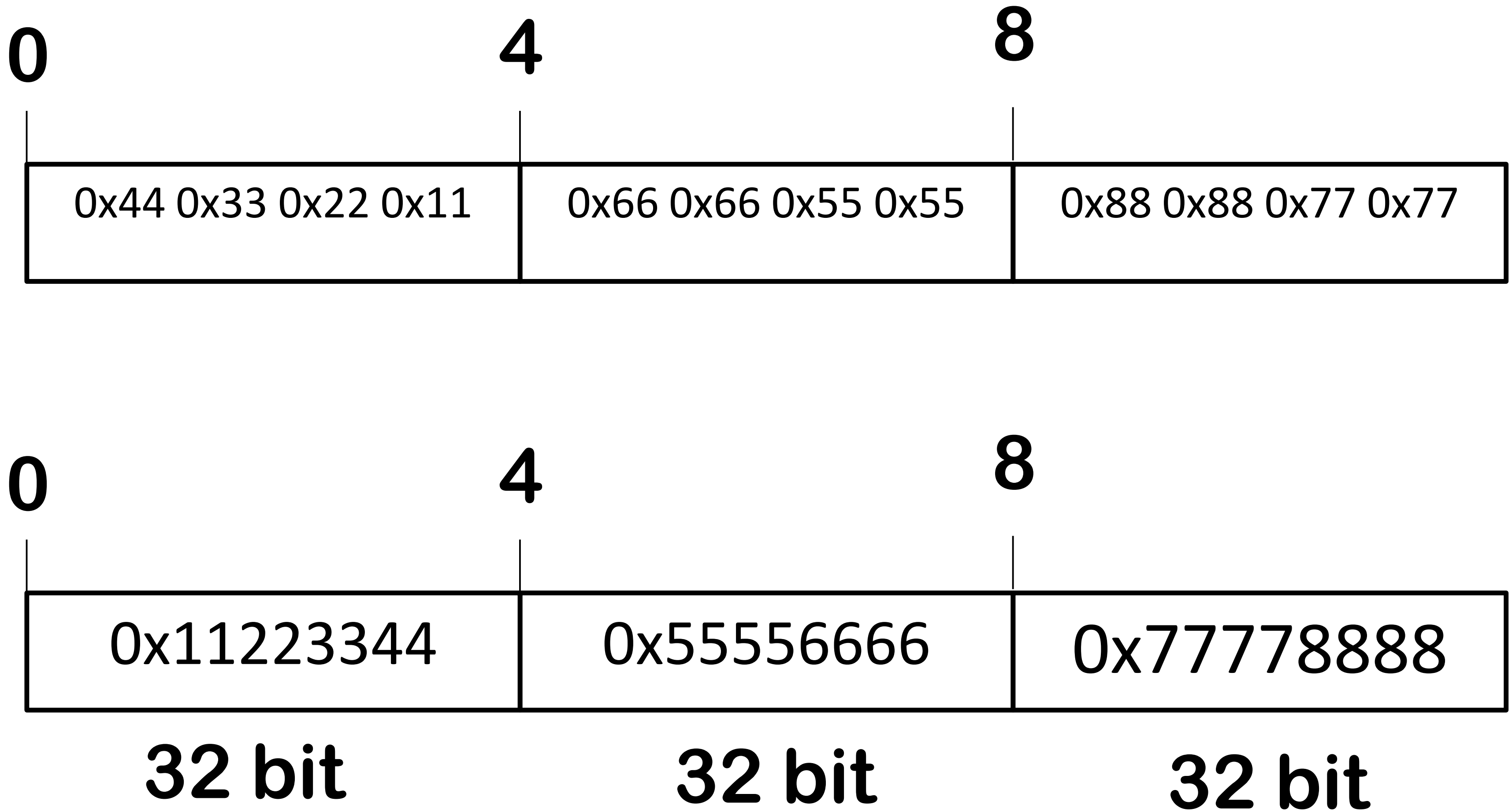
32 bit = 4 bytes

32 bit = 4 bytes

32 bit = 4 bytes



Numbers in memory



ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

ASCII - Hexdump

```
0008b400  25 00 e9 cc fd ff ff 66  0f 1f 84 00 00 00 00 00  |%......f........|
0008b410  e8 2b 21 01 00 e9 c4 fe  ff ff 66 0f 1f 44 00 00  |.+!.......f..D..|
0008b420  44 3b 2d f1 fe 25 00 0f  8f 5f fe ff ff 8b 05 d5  |D;-..%..._......|
0008b430  fe 25 00 3b 05 fb fd 25  00 0f 8d 4d fe ff ff 83  |.%.;...%...M....|
0008b440  c0 01 89 05 c0 fe 25 00  e9 3f fe ff ff 0f 1f 00  |......%..?......|
0008b450  41 57 41 56 41 55 49 89  fd 41 54 55 53 48 83 ec  |AWAVAUI..ATUSH..|
0008b460  08 8b 1d cd fd 25 00 8b  6f 20 8d 43 01 4c 63 e3  |.....%..o .C.Lc.|
0008b470  89 ef 89 2d b8 dd 25 00  89 05 b6 fd 25 00 48 8b  |...-..%.....%.H.|
```

Numbers in memory

Recap:

- Numbers can be displayed in decimal, or hex (0-9, a-f)
- Numbers are stored as 16, 32 or 64 bit value as little endian
- If we look at little endian numbers as bytes, they are inverted
- If we look at numbers in memory, we can’t know if they are 8, 16, 32 or 64 bit
- We can try to interpret bytes as ASCII

Operating System Basics

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

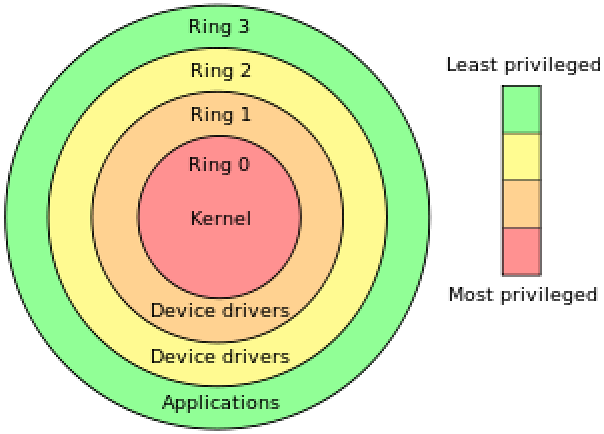
OS Basics: Rings

Ring 0: Kernel (Kernelspace)

- Not covered here
- Can be interacted with by using “syscalls”

Ring 3: Userspace

- Where all programs run
- ls, Bash, Vim, Apache, Xorg, Firefox, …



How to transit from userspace to kernelspace?

- System Calls (syscall)

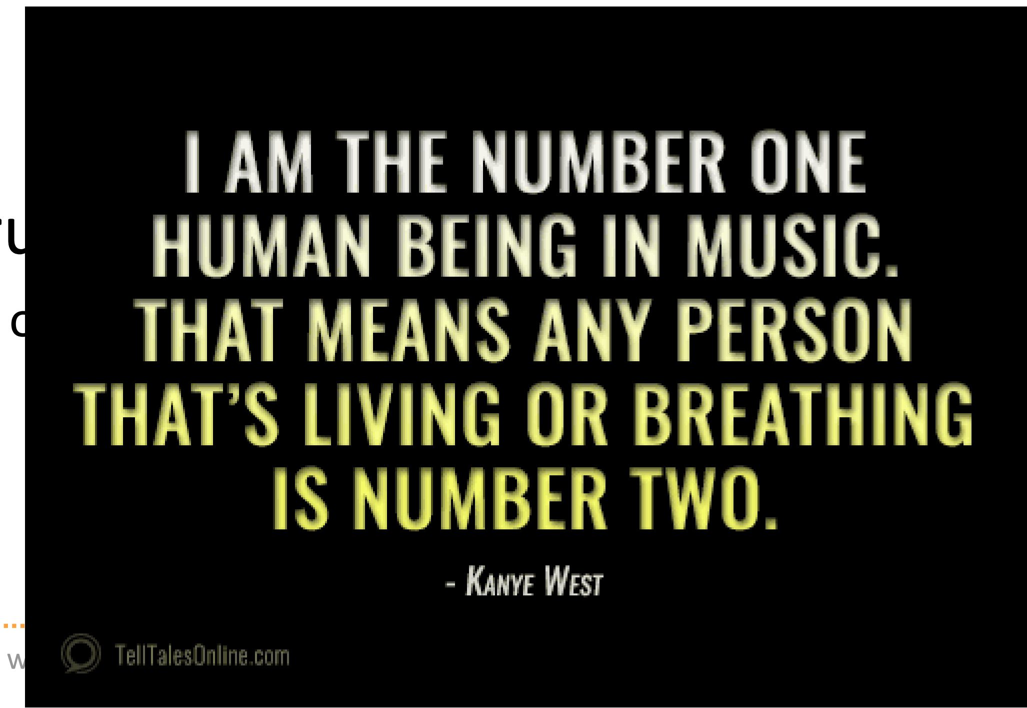
OS Basics: Rings

A Process:

- Is a running program
  - Program lives on disk (static)
  - Process lives on memory (alive)
- Process thinks he “owns” the hardware
  - RAM
  - CPU

Multiple processes can ru

- Everyone thinks he is the c
- Like Kanye West



OS Basics: Process and Memory

Processes can address:

- **4 GB of memory** in 32bit OS
  - (2-3 GB actually)

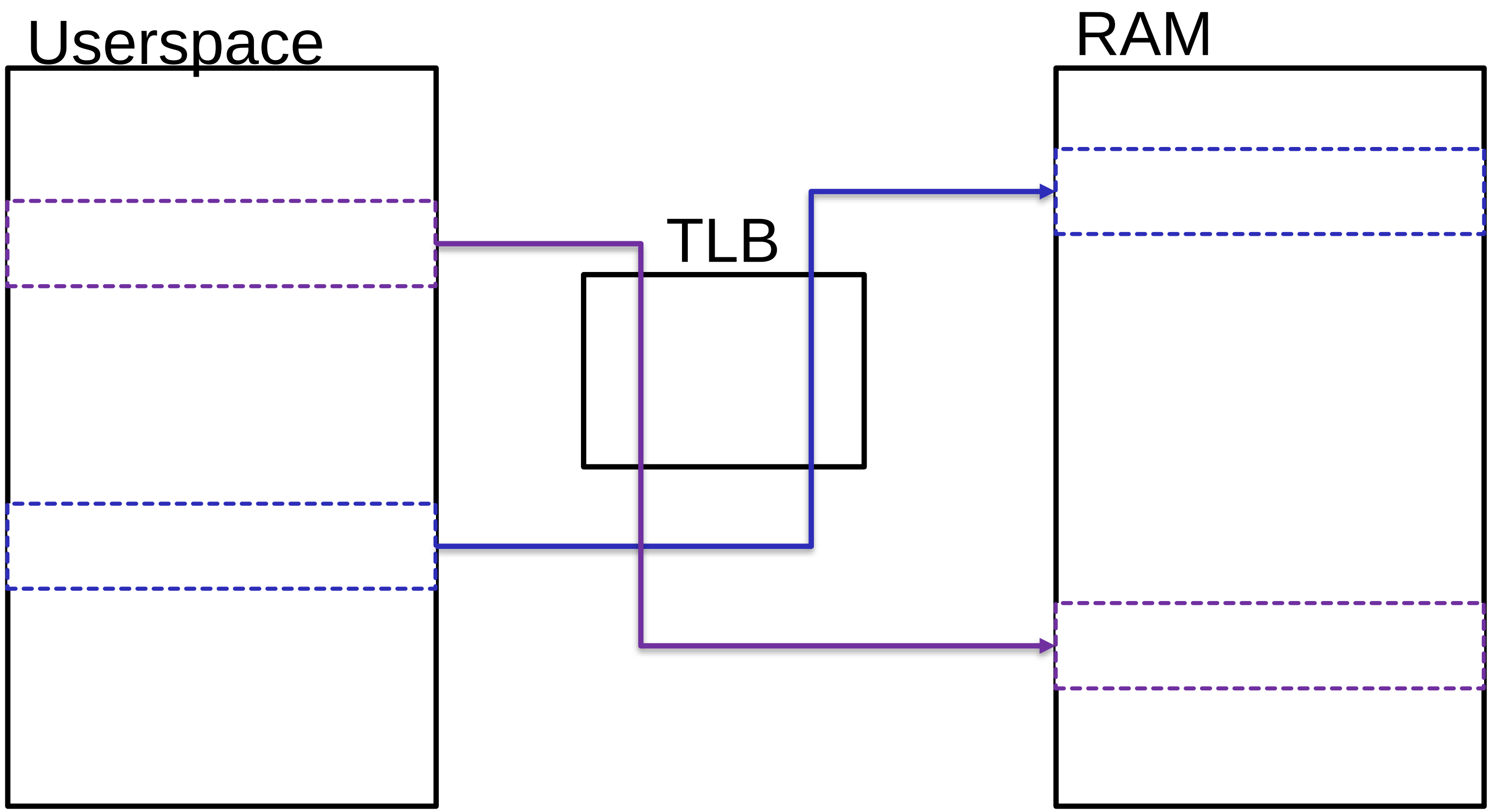
- Independent on how much memory there really is

What if we have:

- Only 2 GB RAM?
  - OOM (Out Of Memory) when too much memory is used
- 8 GB RAM?
  - 2 Processes can use all their 4GB!

OS Basics – Kernelspace/Userspace

OS/CPU manages mapping between physical pages and process (virtual) pages

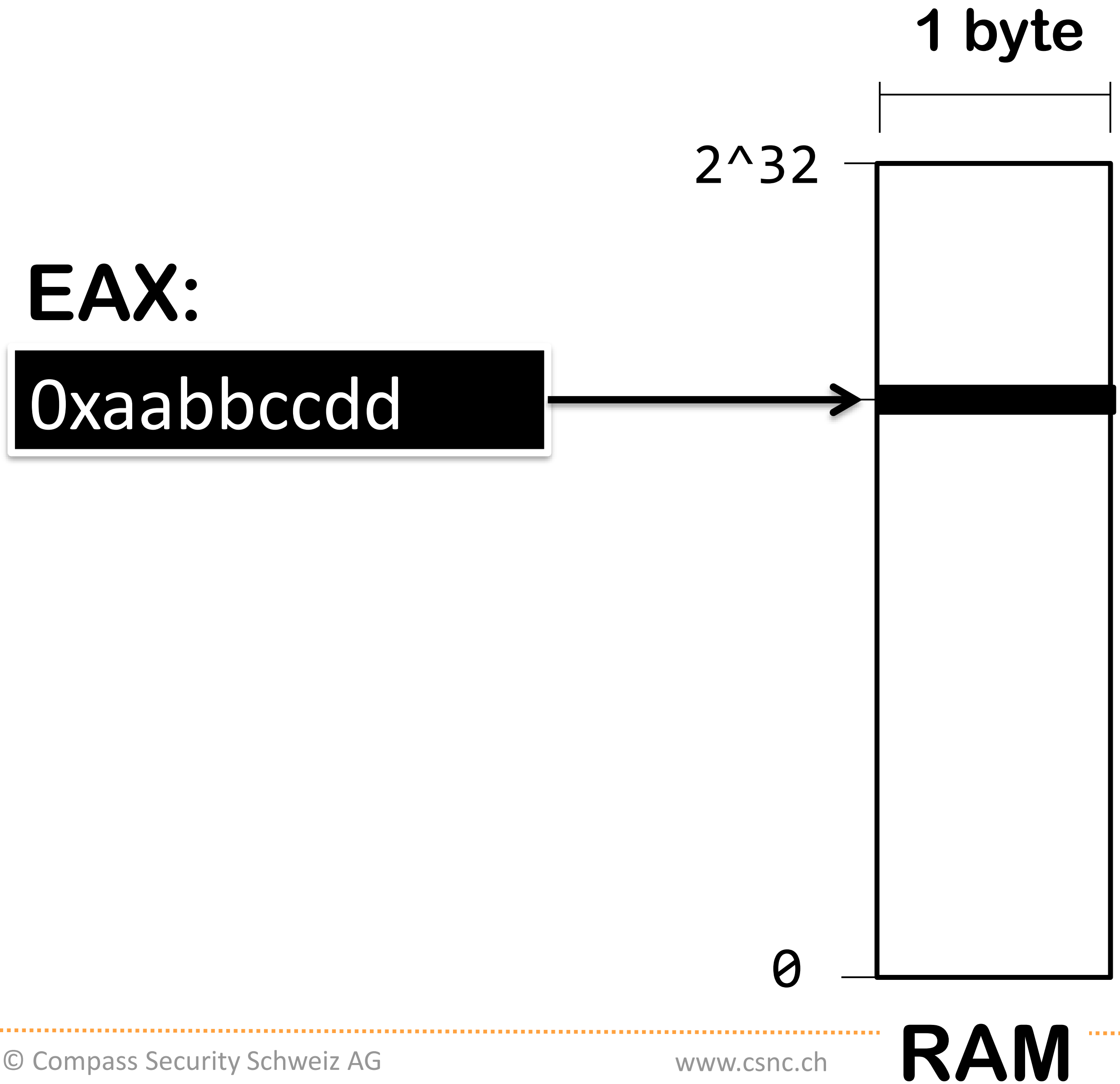


Why 4 GB?

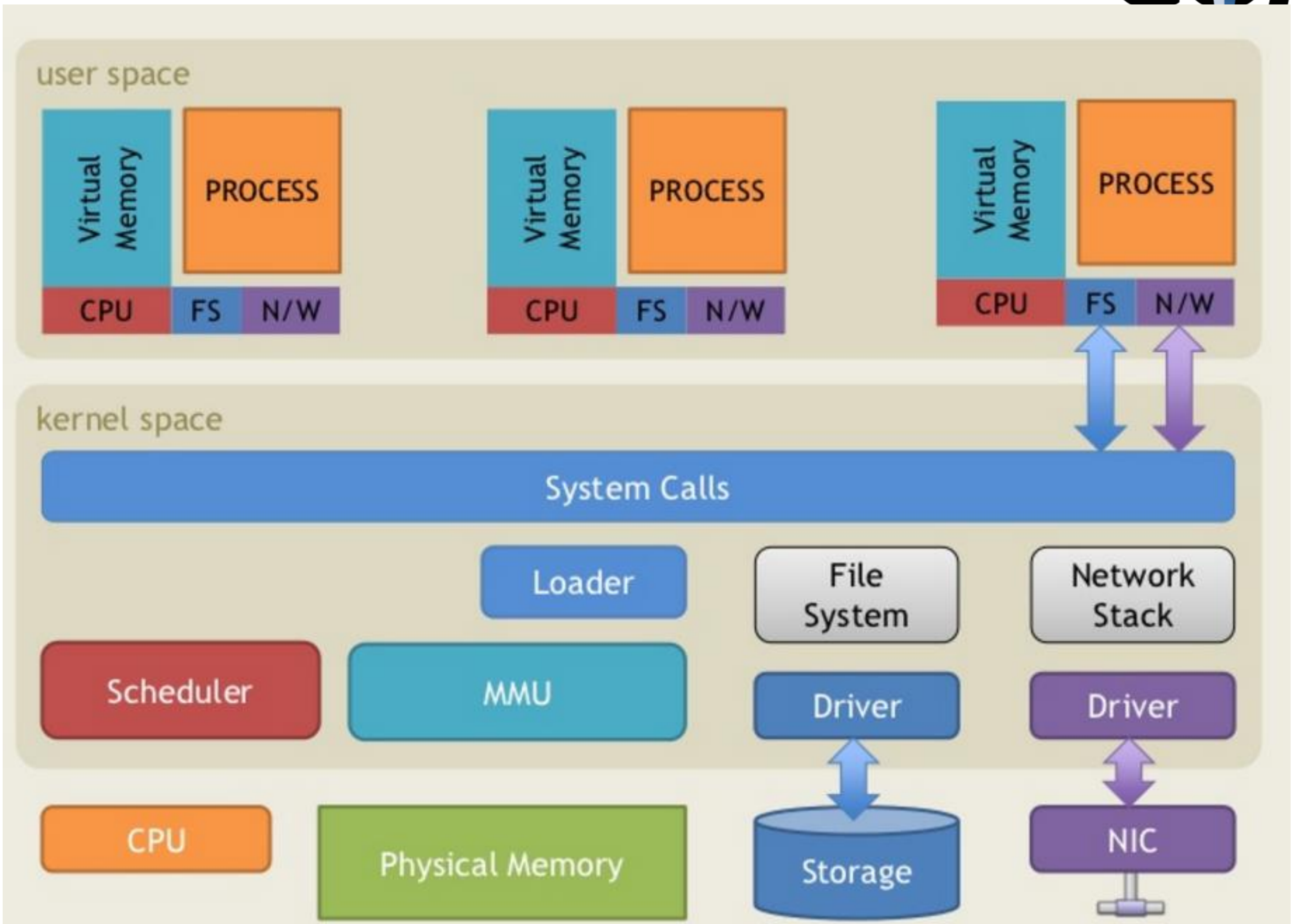
- 32 bit register
- Register are used to address memory
- 2^32 = 4 billion = 4 gigabyte

A process has therefore access to **4 billion one-byte** memory locations

OS Basics: Process and Memory



OS Overview

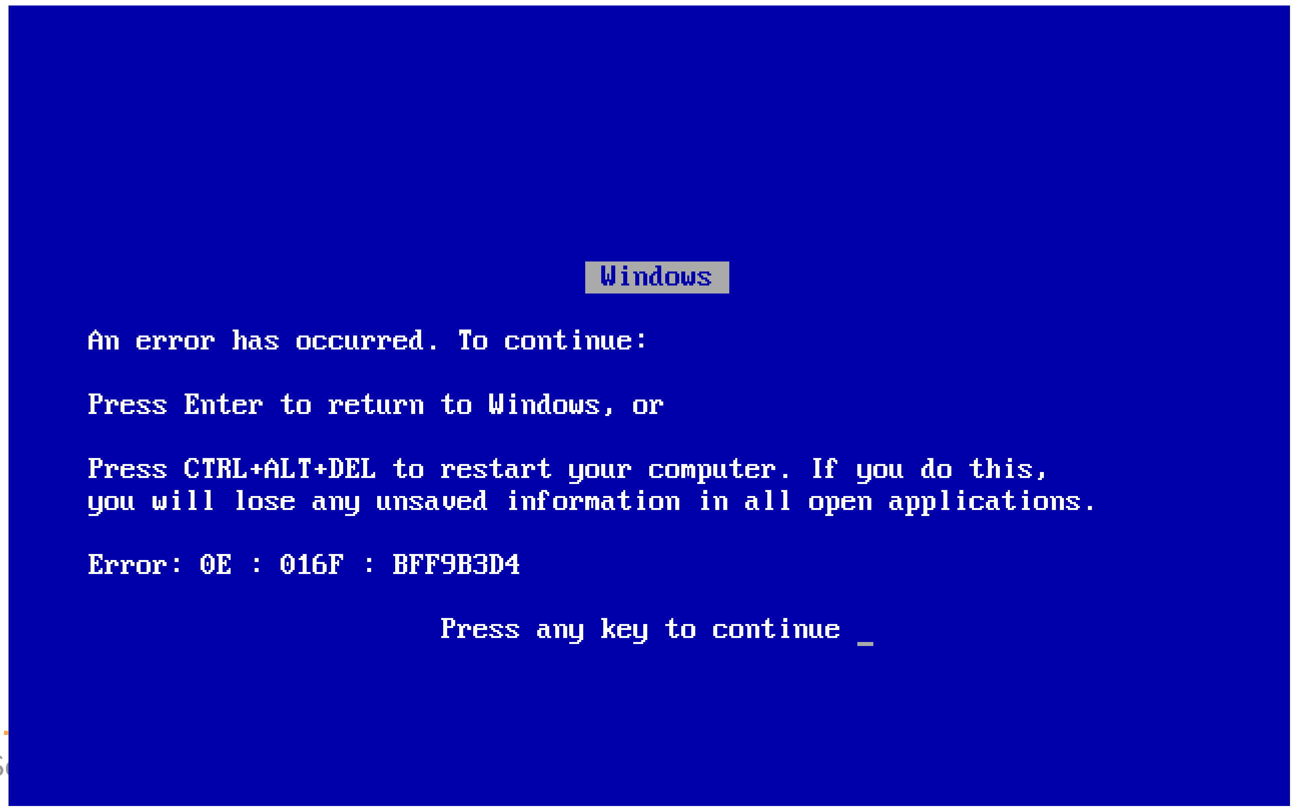


http://www.slideshare.net/saumilshah/operating-systems-a-primer

OS Overview

History lesson: “The good old times”

- Windows did not have true protected memory until windows NT/2000
  - Including all of DOS, Windows 3.1, Windows 95, 98, ME
- Every process could write into all all other processes, or even the OS
- “Blue screen of death”



There's only one CPU, how can:

- Multiple programs run at the same time?
- The OS and the programs run at the same time?

Solution: Interrupts

- Timer interrupts
- Interrupts are handled by the kernel
  - Time / clock
  - Network interface
  - USB devices
- Kernel schedules the different processes

OS Overview

Recap:

- Processes are programs which are alive in the RAM
- Every process thinks he owns the computer (including all the RAM)
- Evey process has access to 2^32 (~4 billion) memory locations of 1 byte size

32 bit vs 64 bit

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

32bit vs 64bit

From 32 to 64 bit

- You all are probably too young for this
- But it was kinda big thing
- AMD invented the current 64 bit architecture
  - Intel wanted a new one: Itanium. Failed hard.
  - (AMD was better than Intel in most respects. Sigh).
- x86 to x64 / amd64
  - 8086, 80286, 80386, 80486, 80586 aka Pentium

- "Is windows 64 bit twice as good/fast than windows 32 bit?"
  - Width of the CPU registers define the amount of addressable memory

32bit vs 64bit

64 bit pros:

- Can address more than 4 gb of memory per computer
- 64 bit calculations are maybe a bit faster

64 bit cons:

- Programs use more space
  - Because pointers and data-types (integer) are twice as big
  - On disk, memory and cache

32bit vs 64bit

64 bit registers are prefixed with “R” (RAX, RIP, …)

New registers: R8-R15

Pointers are 64 bit

Push/Pop are 64 bit

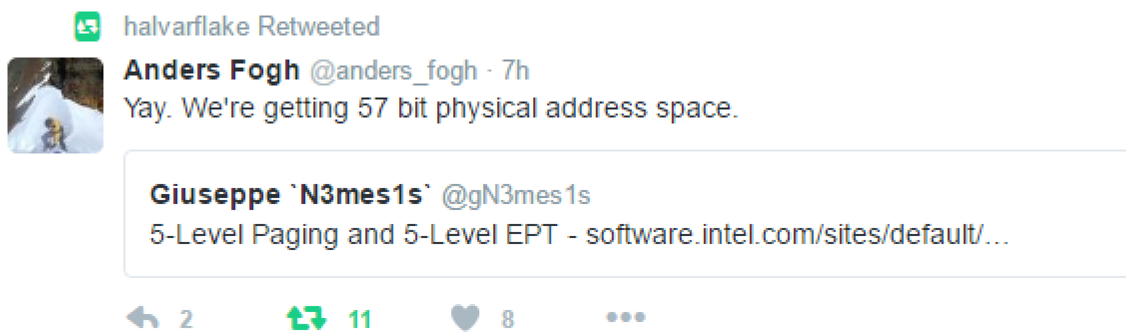
For 64 bit:

- 64 bit are 18 exabytes
- Only 47 bit are used (=140 terabytes)
- < `0x00007fffffffffff`

32bit vs 64bit

For 64 bit:

- 64 bit are 18 exabytes
- Only 47 bit are used (=140 terabytes)
- `< 0x00007fffffffffff`



5-Level Paging and 5-Level EPT

White Paper

Revision 1.0

December 2016

32bit vs 64bit

Linux (and Windows) can execute 32 bit processes on a 64 bit OS

- C:\Program Files
- C:\Program Files (x86)

- /lib/lib
- /lib/lib64

The 32 bit process does not realize he’s on a 64 bit system

- But needs a 32 bit runtime

For this presentation:

32 bit is “old” and “dead”

- But its much easier to create and explain exploits in it

Old plan was: “Lets be modern, 64 bit only”

Current plan: “Lets be modern, but still use 32 bit to exploit stuff”

Sorry…

32bit vs 64bit

Recap

- There are some differences between 32 and 64 bit
- A 32 bit process can run on a 64 bit system as 32 bit

Videos

https://media.ccc.de/v/34c3-9064-the_ultimate_apollo_guidance_computer_talk

https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEFCON-25-Christopher-Domas-Breaking-The-x86-ISA.pdf