Virtualization on x86 Architecture

Jacob Lammert Vladimir Spassov

Bauhaus-Universität Weimar

04.11.2021

Contents

1. Introduction
   - Processors at our disposal
   - IA_32 System Architecture Overview
   - Processor Modes
   - Hierarchy of Right
2. x86 VMX
   - Basics
   - VMX Instructions
   - VMX Right Levels
   - VMX Life Cycle
   - Importent Bits
3. Recommendations for the Project

Introduction

CPU Name	total cores	VT-x	base frequency
Intel® Core™ 2 Quad Q8400	4	yes	2,66 Ghz
Intel® Pentium ® 4	1	no	2,6 Ghz
Intel® Core™i5-10500	6	yes (with EPT)	3,1 Ghz

Figure: **Processors at our disposal**

Introduction

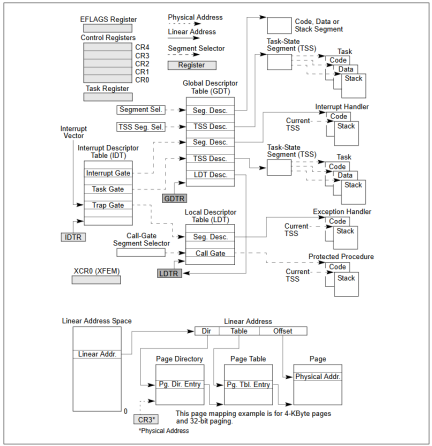

Figure: IA_32 System Architecture [3]

Introduction

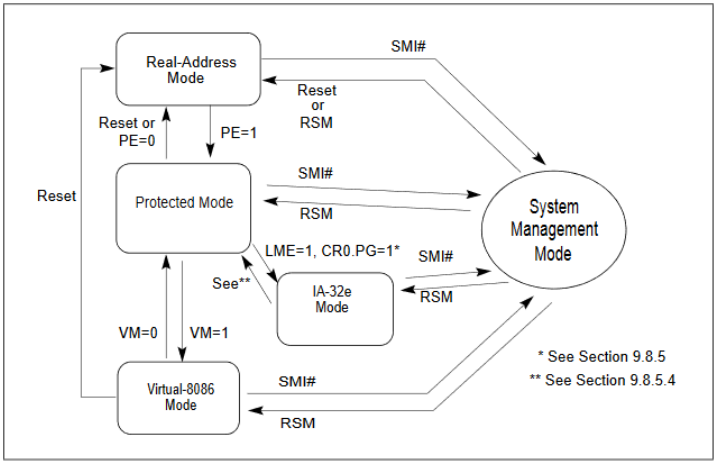

Figure: Processor Modes [3]

Introduction

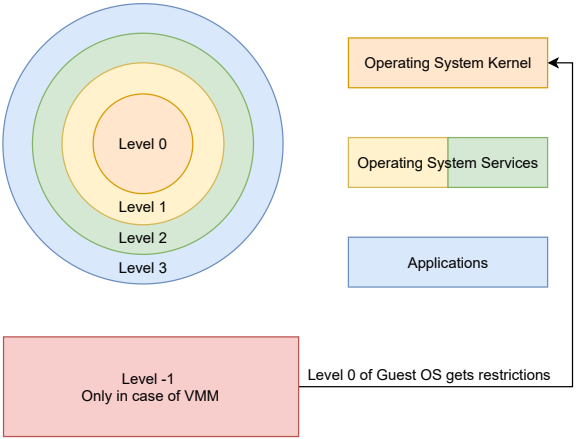

Figure: Hierarchy of Rights

x86 VMX [3]

- basics of virtual machine architecture
- overview of the virtual-machine extensions(VMX)

x86 VMX (basics) [3]

Virtual-machine monitors (VMM):

- host with full control of the processor
- A VMM presents guest software with an abstraction of a virtual processor and allows it to execute directly on a logical processor.
- can retain selective control of processor resources, physical memory, interrupt management, and I/O.

Guest software:

- virtual machines can run independently on the same hardware
- the guest software runs with a lower privilege than the VMM (VMM keeps control over certain platform resources)

x86 VMX (instructions) [3]

VMX operations

- VMX root operation - standard for VMM
- VMX non root operation - standard for guest software

VMX transitions - transition between VMX non-root and VMX root operation

- VM entries - from root to non-root
- VM exits - from non-root to root

x86 VMX (instructions) [3]

Intel/AMD Mnemonic
INVEPT
INVVPID
VMCALL
VMCLEAR
VMFUNC
VMLAUNCH
VMRESUME
VMLAUNCH
VMRESUME
VMPTRLD
VMPTRST
VMREAD
VMWRITE
VMXOFF
VMXON

Figure: Basic VMX instructions [7]

x86 VMX (rights)

VMX root

- New instructions (all VMX instructions) available.
- Certain other registers get limited.

VMX non-root

- certain instructions (including the new VMCALL instruction) and events cause VM exits
- functionality of software in VMX non-root operation is limited
- only VMM keeps control of real resources
- No bit visible to software indicating that the processor is in VMX non-root operation

x86 VMX (life cycle) [3]

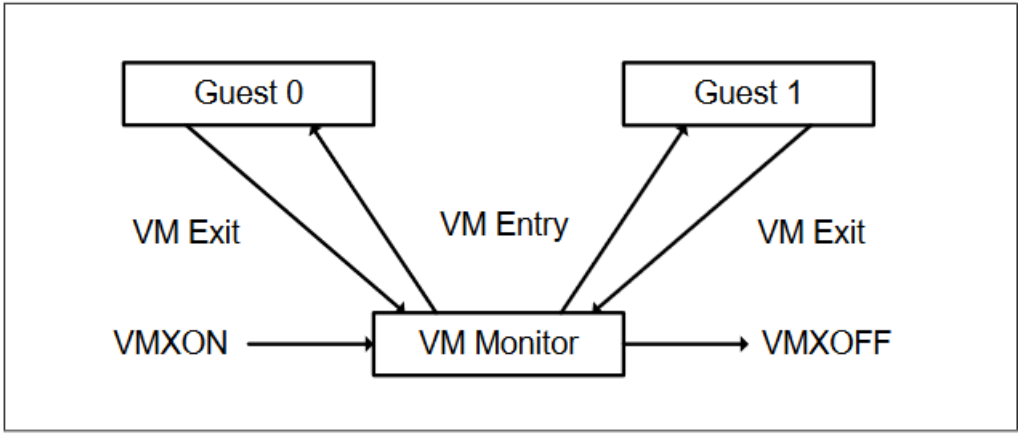

Figure: Interaction of a Virtual-Machine Monitor and Guests [3]

x86 VMX (life cycle) [3]

1. Software enters VMX operation with VMXON instruction
2. with VMLAUNCH and VMRESUME the VMM effects the VM entry, with VM exit the VMM regains control
3. VMM can take action appropriate to the cause of the VM exit end return to the VM with VM entry
4. with VMXOFF the VMM shuts itself down and leaves VMX operation

x86 VMX (importent bits) [3]

- CR4.VMXE[bit 13] must be 1 for execution of VMXON.
- CR4.VMXE can not be cleared in VMX operation.
- Probably? also 12 Bit of IA32_EFER_MSR (Extended Feature Enable Register)
- IA32_EFER_MSR available only in IA32e mode

x86 VMX (important bits)

CR4

Bit	Label	Description
0	VME	Virtual 8086 Mode Extensions
1	PVI	Protected-mode Virtual Interrupts
2	TSD	Time Stamp Disable
3	DE	Debugging Extensions
4	PSE	Page Size Extension
5	PAE	Physical Address Extension
6	MCE	Machine Check Exception
7	PGE	Page Global Enabled
8	PCE	Performance-Monitoring Counter enable
9	OSFXSR	Operating system support for FXSAVE and FXRSTOR instructions
10	OSXMMEXCPT	Operating System Support for Unmasked SIMD Floating-Point Exceptions
11	UMIP	User-Mode Instruction Prevention (if set, #GP on SGDT, SIDT, SLDT, SMSW, and STR instructions when CPL > 0)
13	VMXE	Virtual Machine Extensions Enable
14	SMXE	Safer Mode Extensions Enable
16	FSGSBASE	Enables the instructions RDFSBASE, RDGSBASE, WRFSBASE, and WRGSBASE
17	PCIDE	PCID Enable
18	OSXSAVE	XSAVE and Processor Extended States Enable
20	SMEP	Supervisor Mode Execution Protection Enable
21	SMAP	Supervisor Mode Access Prevention Enable
22	PKE	Protection Key Enable
23	CET	Control-flow Enforcement Technology
24	PKS	Enable Protection Keys for Supervisor-Mode Pages

Figure: Control Register 4[1]

Recommendations for the Project

Our Problems

- University does not provide modules for OS development, Assembler etc.
- Learning ourselves is possible, but a certain amount of time and effort will be needed
- we do not have that much time in our project

Recommendations for the Project

1. Formulating final product as specific as possible (concept, sub-goals)
2. Determine needed Skills (OS dev, IP/TCP Protocol writing, C etc.)
3. Forming Groups for learning necessary skills
4. Learn Skills
5. Implement one sub-goal bye one
6. Sub-Goals we do not manage to achieve can be shoved into next project (BlueP II or so)

Why?

- Because necessary knowledge is very very complex
- Minimisation of knowledge we need to acquire in one step will be important

Quellen I

[1] *CR4*. URL: https://wiki.osdev.org/CPU_Registers_x86.

[2] Dennis Fisher. *China-Linked Hackers Found Using UEFI Rootkit*. URL: https://duo.com/decipher/china-linked-hackers-found-using-uefi-rootkit.

[3] *Intel® 64 and IA-32 Architectures Sodtware Developer´s Manual, Volume 3 (3A, 3B, 3C & 3D): System Programming Guide*. Tech. rep. 325384-075US. Intel Corporation, June 2021.

[4] *Intel® 64 and IA-32 Architectures Software Developer Manuals*. URL: https://www.intel.com/content/www/us/en/developer/articles/technical/intel-sdm.html.

[5] *Technical Resources: Intel® Core™ Processors*. URL: https://www.intel.com/content/www/us/en/products/docs/processors/core/core-technical-resources.html.

Quellen II

[6] Zack Whittaker. *Scranos, a new rootkit malware, steals passwords and pushes YouTube clicks*. Apr. 2019. URL: https://techcrunch.com/2019/04/16/scranos-rootkit-passwords-payments/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKW0JKrj_E8LGEPB6Ht-Gp8S9ey8LzyfFq0PfONvkNGBAsIV9zW8UP9puIEzuOg4cXUhkSGJtLHW7D1aIBgjljrxPDxfNgx AG609YE3d0BFSua0vrEtnFwE2mzW24FZAHzNDi8eHTvRv1gxz.

[7] *x86 Assembly Language Reference Manual - 3.34 VMX Instructions*. Nov. 2020. URL: https://docs.oracle.com/cd/E37838_01/html/E61064/gntbx.html.