Überblick über die Intel Virtualization Technology

Thilo Vörtler

s7933688@mail.inf.tu-dresden.de

Gliederung

- Einleitung
- Hardware Virtualisierung
- Intel Virtualization Technology
- Zusammenfassung/Ausblick

Virtualisierungsebenen

- Was versteht man unter Virtuellen Maschinen?
  1. Virtualisiertes Betriebssystem, welches es ermöglicht mehrere Betriebssysteme auf einem System auszuführen.
  2. Ein abstraktes Computer-System wie es Java oder C# bieten. Diese Virtuellen Maschinen erlauben es Code auf Systemen mit unterschiedlichen Betriebssystem auszuführen.
  3. Ein emuliertes Computersystem, welches Code von Systemen ausführt die noch nicht oder nicht mehr existieren.

Virtualisierungsebenen

- Hardware-level virtualization
- Operating system–level virtualization
- High-level language virtual machines

Anforderungen und Probleme

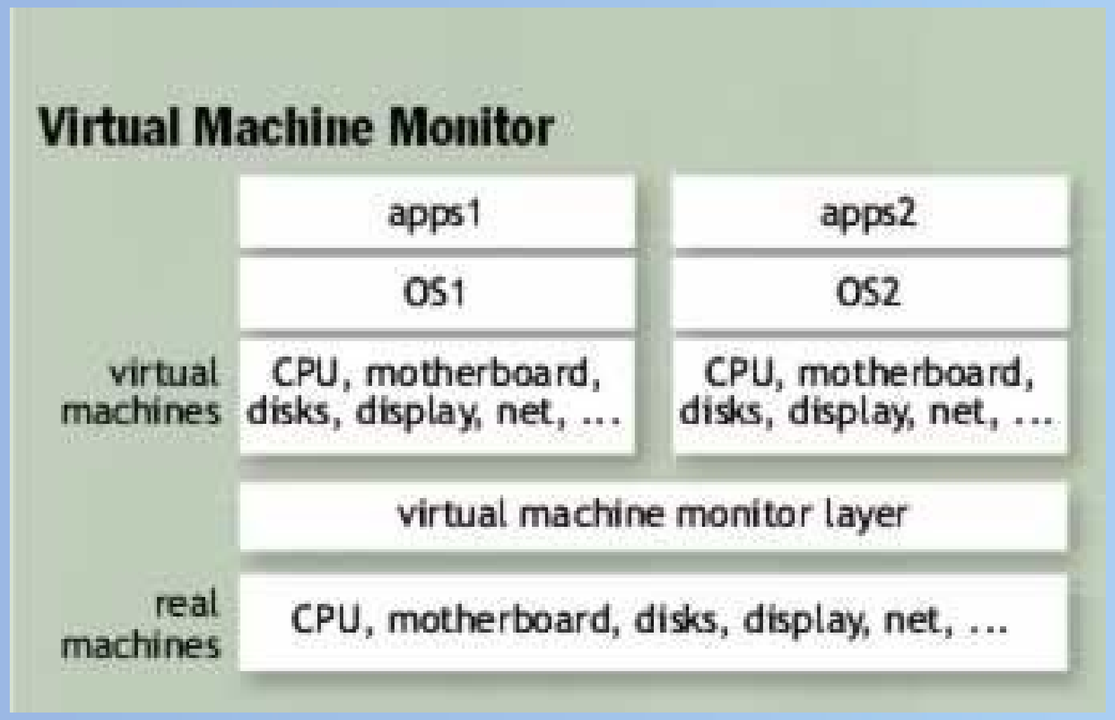
- Anforderungen an Virtuelle Maschinen
  - Software Kompatibilität
  - Isolation
  - Kapselung
  - Performance

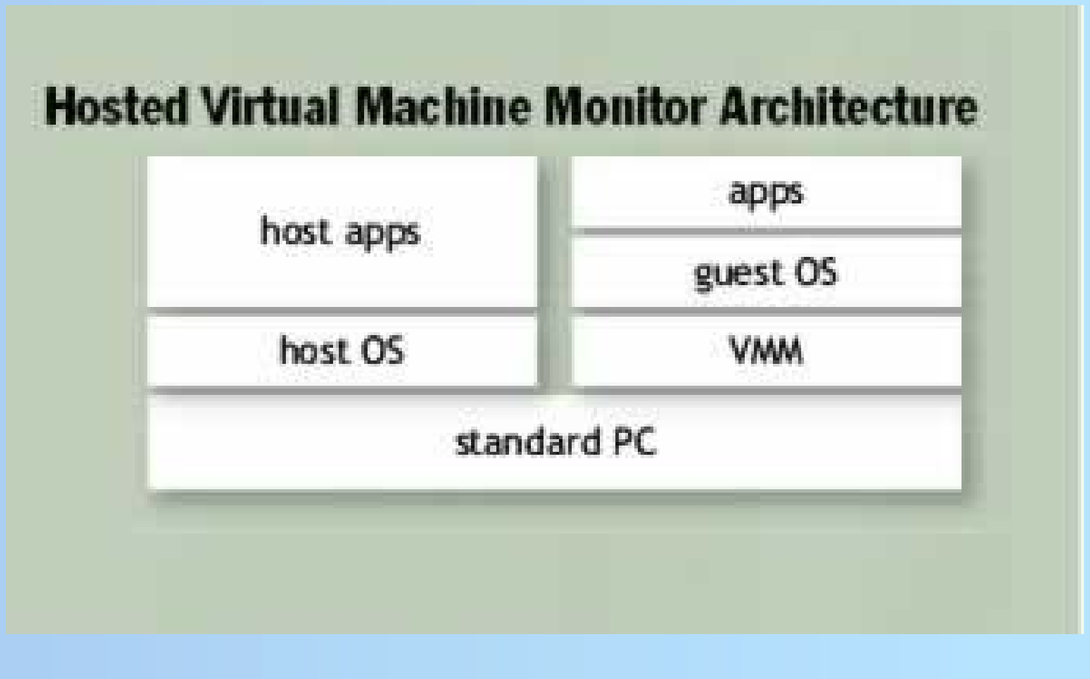
- Probleme aller Virtualisierungslösungen
  - Die Zielumgebung muss genau reproduziert werden
  - Es muss die Umgebung, die die Software erwartet nachgebildet werden (insbesondere Zeit- und I/O-Verhalten)
  - Es muss eine nutzbare Performance erreicht werden

Geschichte

- VMM:
  - Virtual Machine Monitor
- 1960/1970 bereits auf IBM Mainframes verwendet (VM/370), dabei wurde Software volle Kontrolle über das System vorgetäuscht
- Danach von Multi-User-Betriebssystemen verdrängt
- Ende der 1990er Jahre durch Hosted Virtual Machines wiederbelebt

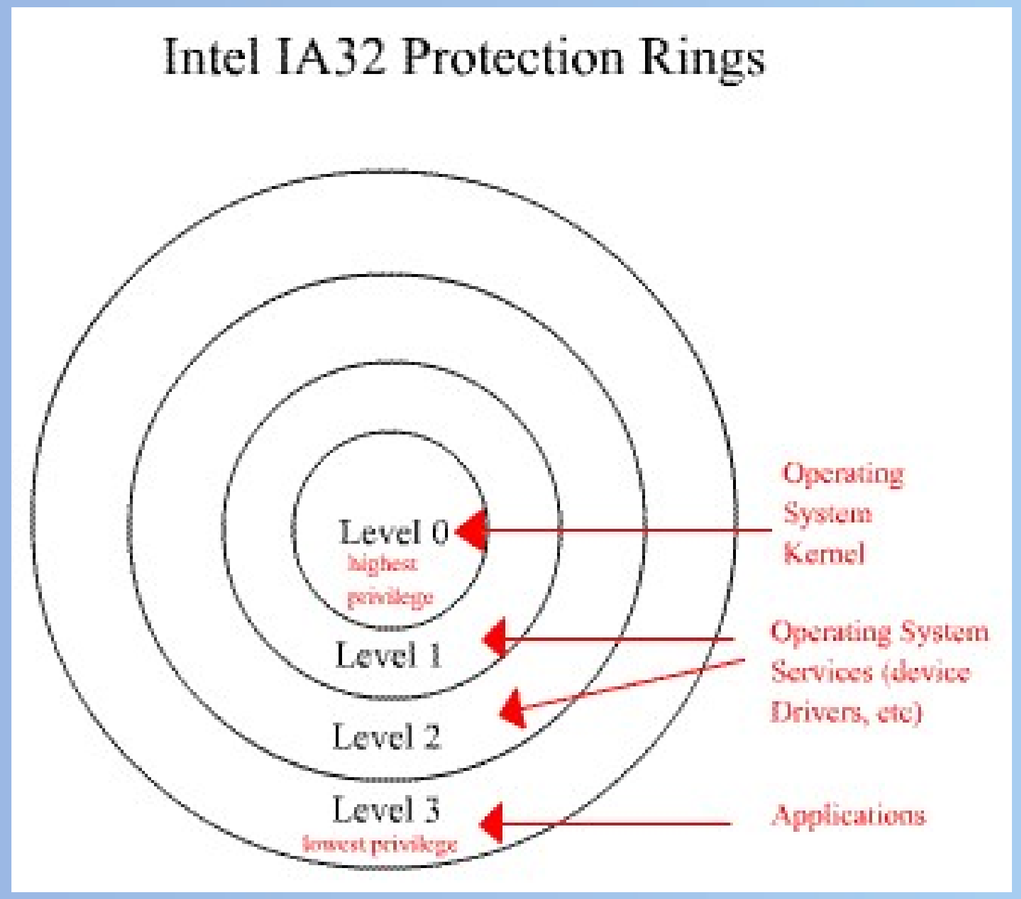
Umsetzungen

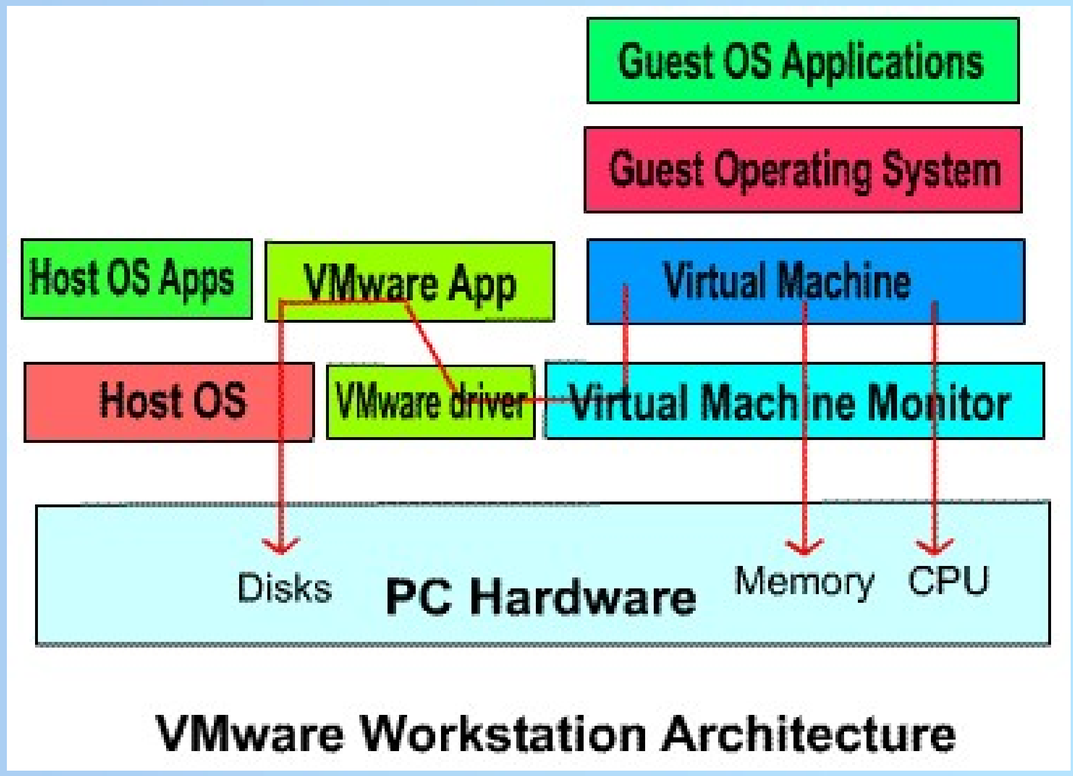




- Bei beiden Varianten sind Eingriffe in das Betriebssystem notwendig

Hosted Virtual Machine

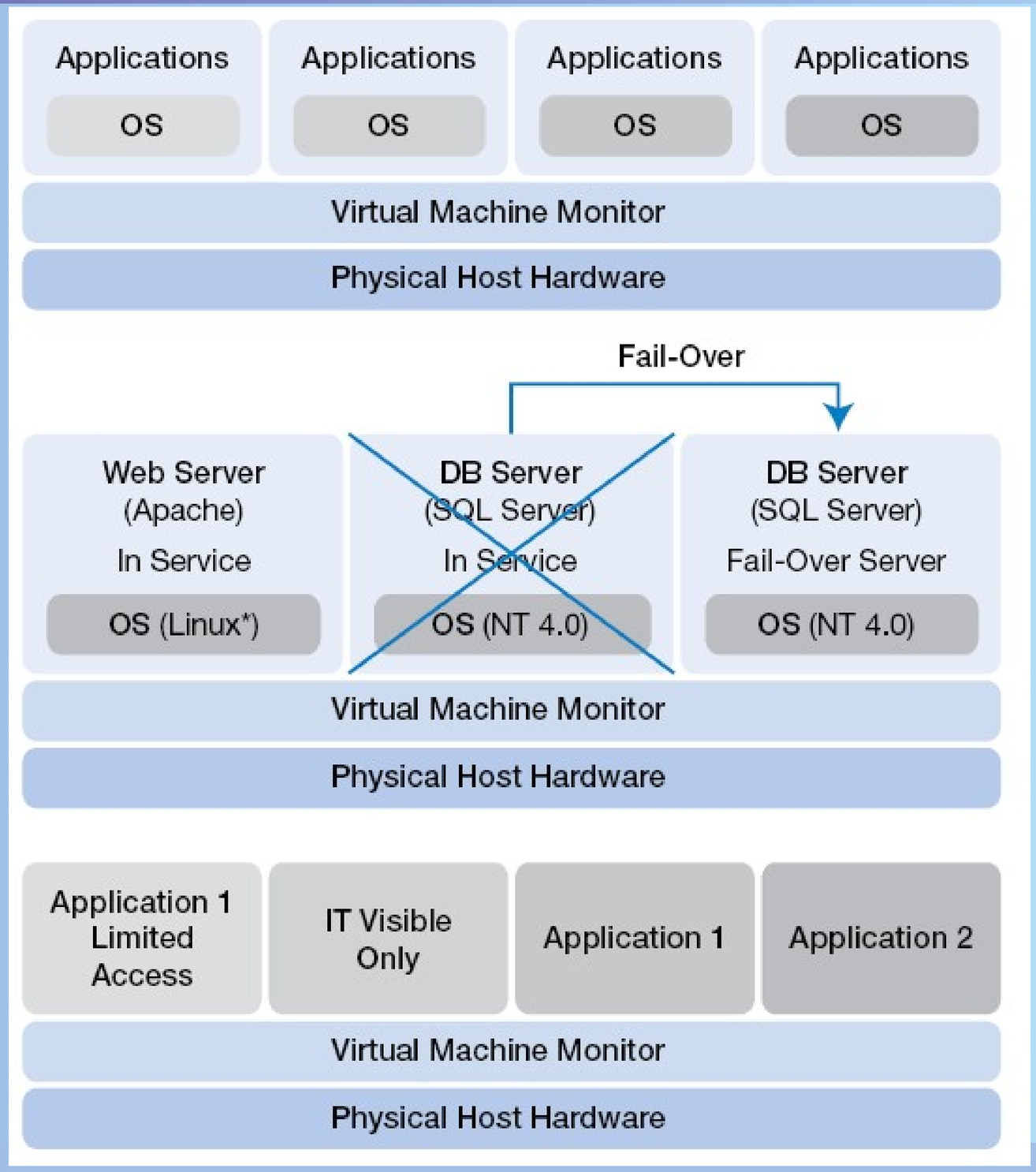




VMware Workstation Architecture

- VMware Workstation und Server
- Microsoft Virtual Server

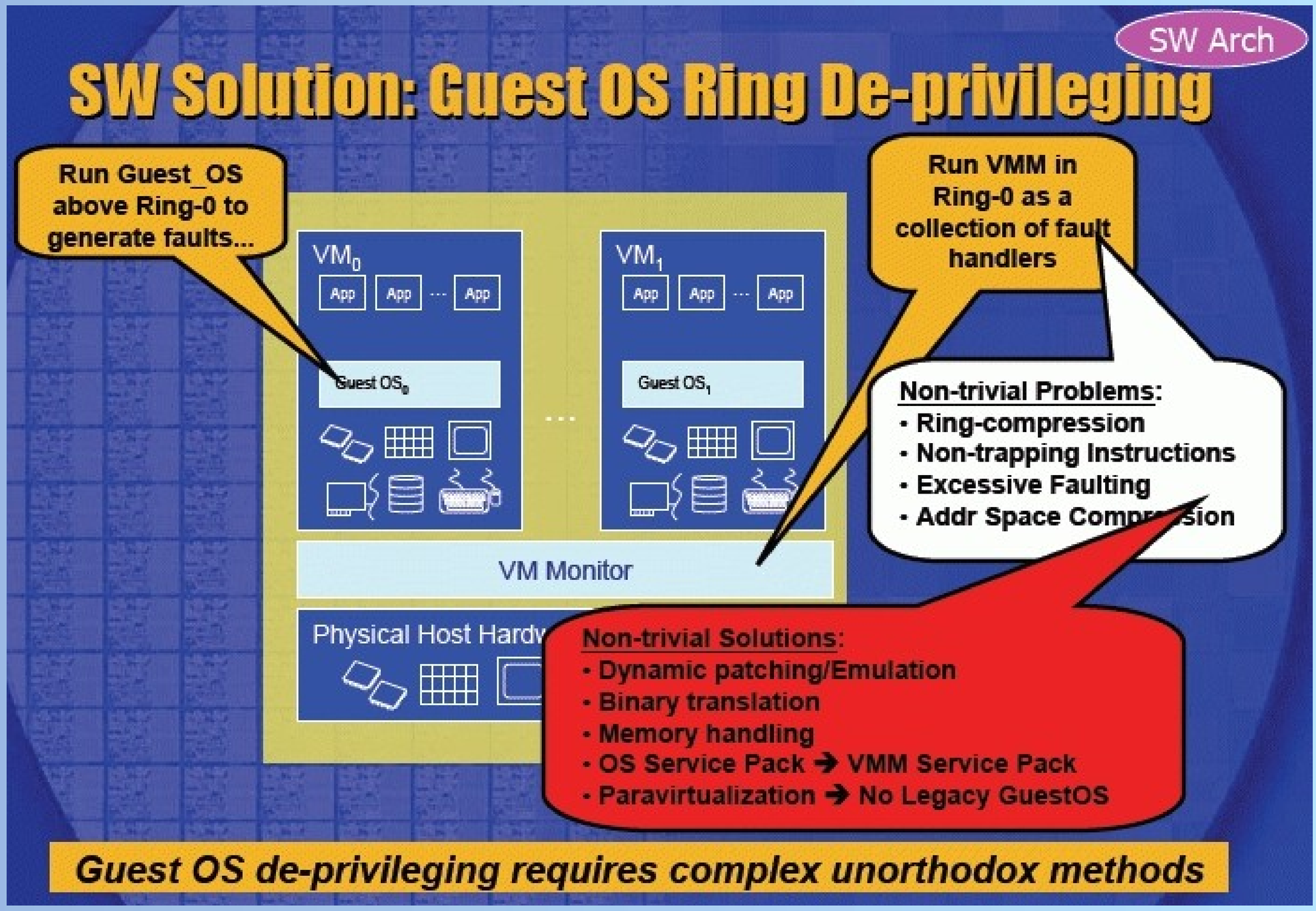
Beispiele


Applications
OS
Applications
OS
Applications
OS
Applications
OS
Virtual Machine Monitor
Physical Host Hardware
Fail-Over
Web Server
(Apache)
In Service
OS (Linux*)
DB Server
(SQL Server)
In Service
OS (NT 4.0)
DB Server
(SQL Server)
Fail-Over Server
OS (NT 4.0)
Virtual Machine Monitor
Physical Host Hardware
Application 1
Limited
Access
IT Visible
Only
Application 1
Application 2
Virtual Machine Monitor
Physical Host Hardware

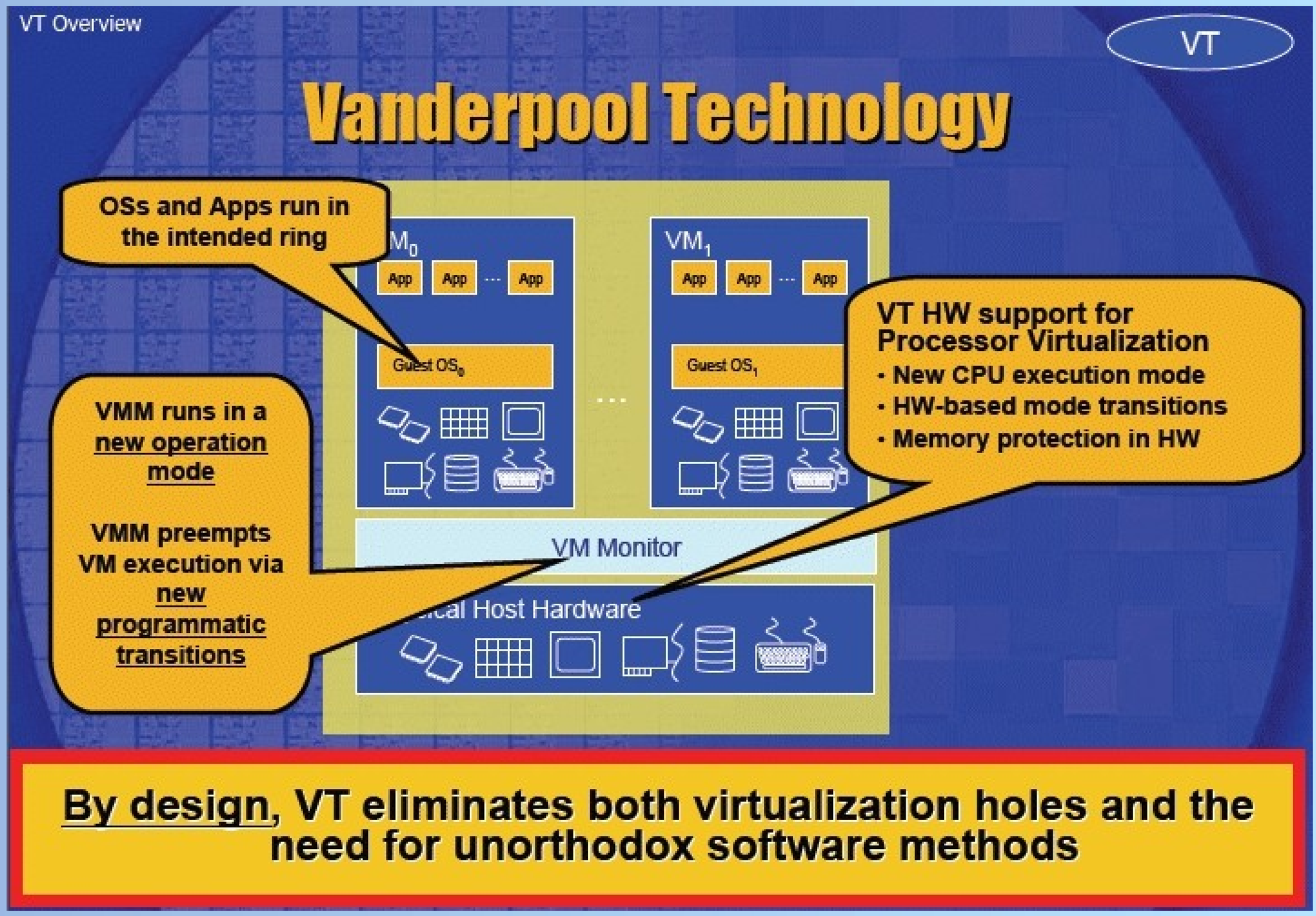
Überblick

- Erstmals 2003 unter dem Namen *Vanderpool* präsentiert
- 2 unterschiedliche Technologien unter den Namen Intel Virtualization Technology
  - Intel Virtualization Technology for the IA-32 Intel Architecture
  - Intel Virtualization Technology for the Intel Itanium Architecture (VT-i)
- Einführung ab zweitem Halbjahr 2005 in Itanium-Prozessoren
- Ab 2006 in Xeon-Prozessoren
- Ab 2005 In Desktop-Prozessoren (Pentium 4)

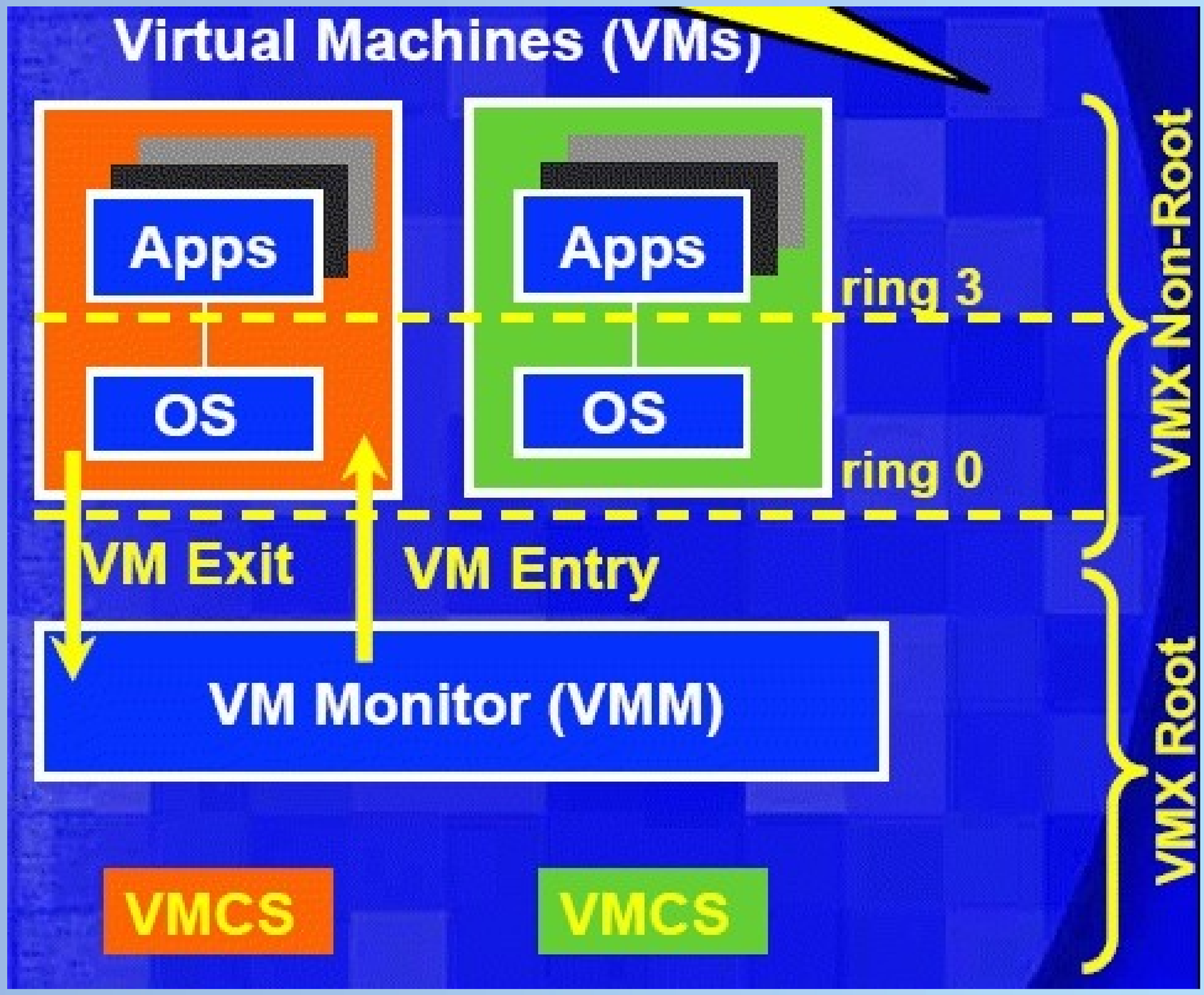
Überblick 1


SW Arch
SW Solution: Guest OS Ring De-privileging
Run Guest_OS above Ring-0 to generate faults...
Run VMM in Ring-0 as a collection of fault handlers
VM0
App
App
App
Guest OS0
VM1
App
App
App
Guest OS1
VM Monitor
Physical Host Hardw
Non-trivial Problems:
• Ring-compression
• Non-trapping Instructions
• Excessive Faulting
• Addr Space Compression
Non-trivial Solutions:
• Dynamic patching/Emulation
• Binary translation
• Memory handling
• OS Service Pack → VMM Service Pack
• Paravirtualization → No Legacy GuestOS
Guest OS de-privileging requires complex unorthodox methods

Überblick 2


VT Overview
VT
Vanderpool Technology
OSs and Apps run in the intended ring
VMM runs in a new operation mode
VMM preempts VM execution via new programmatic transitions
VM0
App
App
App
Guest OS0
VM1
App
App
App
Guest OS1
VM Monitor
Host Hardware
VT HW support for Processor Virtualization
• New CPU execution mode
• HW-based mode transitions
• Memory protection in HW
By design, VT eliminates both virtualization holes and the need for unorthodox software methods

Überblick 2


Virtual Machines (VMs)
Apps
OS
Apps
OS
ring 3
ring 0
VMX Non-Root
VM Exit
VM Entry
VM Monitor (VMM)
VMX Root
VMCS
VMCS

VMCS Datenstruktur

- VMCS: Virtual Machine Control Structure
- Verwaltet Übergänge zwischen Root und Non-Root Modus
- 4 Kbyte großer Bereich pro virtueller Maschine
- Wird über VMCS-Pointer referenziert (64–Bit Adresse)
- Unterteilt in Guest-State Area, Host-State Area,VM-Execution Control Fields, VM-Exit Control Fields, VM-Entry Control Fields und VM-Exit Information Fields
- Prozessorstatus wird z.B bei VM-Exit in Guest State Area gespeichert

Befehle die VMX Operationen ermöglichen

- VMCALL
  - Aufruf des VMM durch Guest Software (VM exit)
- VMLAUNCH
  - Start einer Virtuellen Maschine (VM entry)
- VMRESUME
  - Wiederaufnahme einer virtuellen Maschine (VM entry)
- VMXOFF
  - Schaltet VMX Befehle ab
- VMXON
  - Aktiviert VMX Befehle

VMX-Befehle zur VMCS Verwaltung

- VMPTRLD
  - Lädt VMCS Pointer
- VMPTRST
  - Speichert VMCS Pointer
- VMCLEAR
  - Setzt den Start Status eines VMCS auf Clear
- VMREAD
  - Speichert eine Komponente des VMCS in einem Zieloperanden
- VMWRITE
  - Liest einen Operanden und speichert diesen in einem VMCS

Zusammenfassung

- Intel VT vereinfacht die Programmierung von Virtualisierungssoftware
- Erster Schritt in einer Reihe von Virtualisierungstechniken (z.B IO Virtualisierung)
- Weiterhin Modifikation von Betriebssystemen notwendig
- Inkompatibel zu AMD‘s Pacifica Technik

Fragen?