Is IT-Virtualisation a Security Panacea?

Frank Ackermann, Dipl. Inf. (FH), CISSP

Agenda

- Virtualisation as a New Trend
- Short Introduction to Virtualisation
- Facts & Threats
- Top 10 Measures
- The Security Concept
- Conclusion

Virtualisation as a New Trend

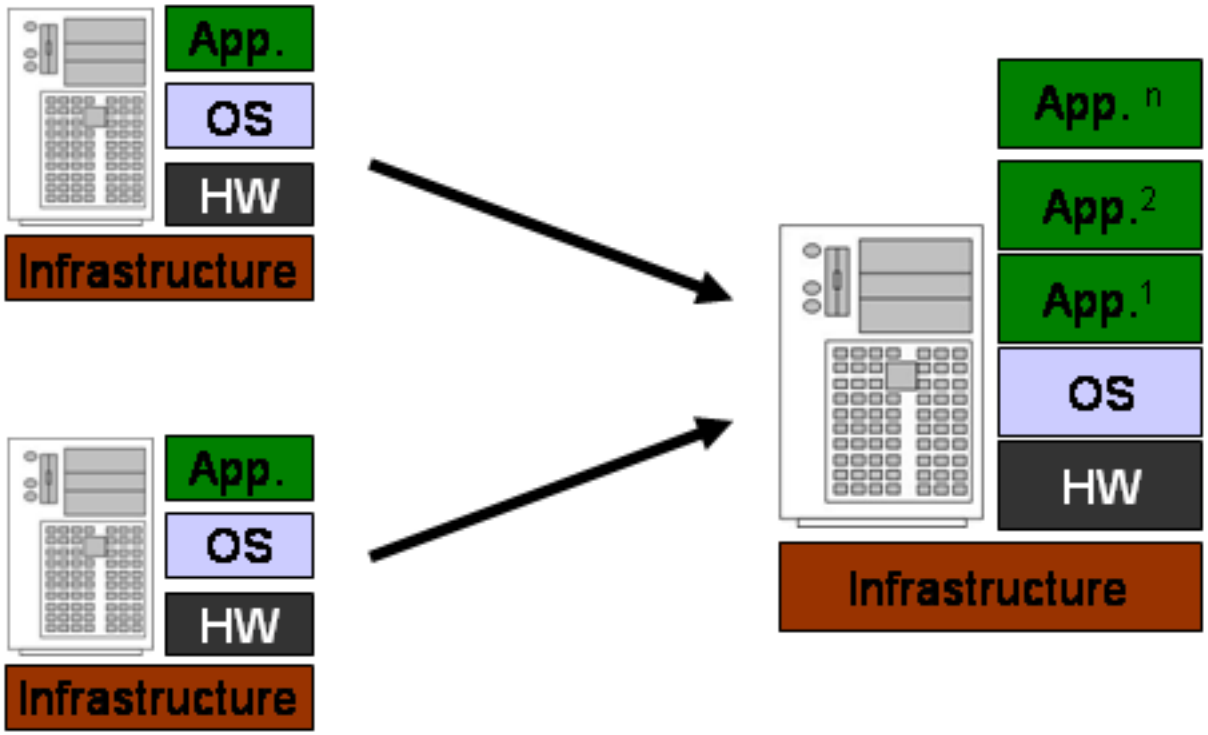
- "**Virtualization, as with any emerging technology, will be the target of new security threats**" said Neil MacDonald, vice president and Gartner Fellow.

  Because of the rush to adopt virtualization for server consolidation efforts, many security issues are being overlooked, best practices are not applied, or in some cases, the tools and technologies for addressing some of the security issues with virtualization are immature or nonexistent. As a result, **through 2009, 60 percent of production VMs will be less secure than their physical counterparts**.

What‘s behind virtualisation and why is IT-security necessary?

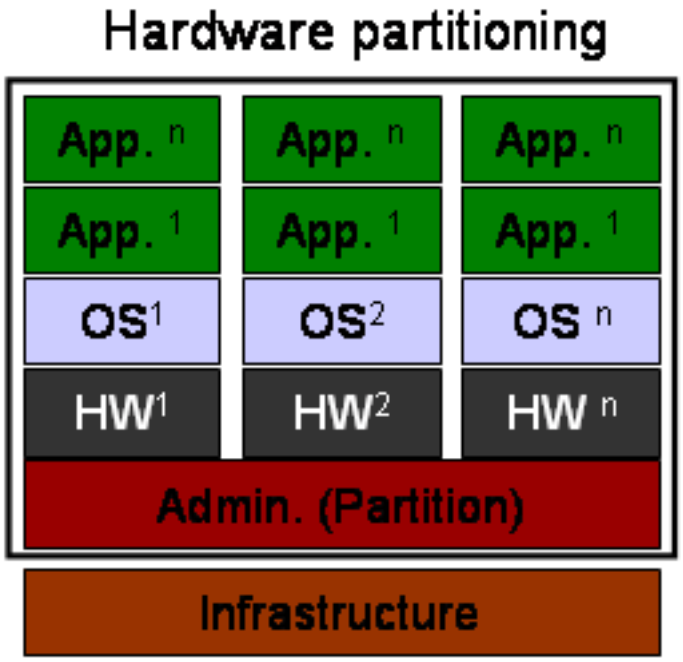
Short Intro to Virtualisation I

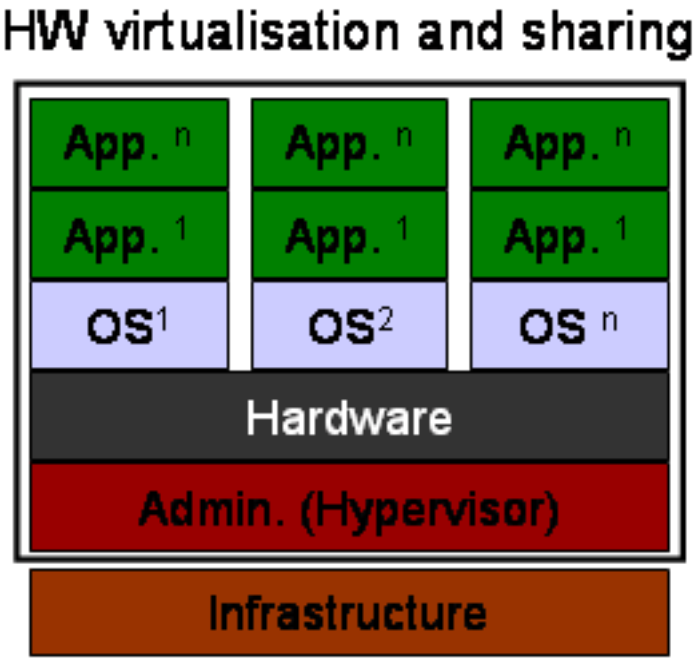
- Consolidation is the basis for virtualisation



Short Intro to Virtualisation II

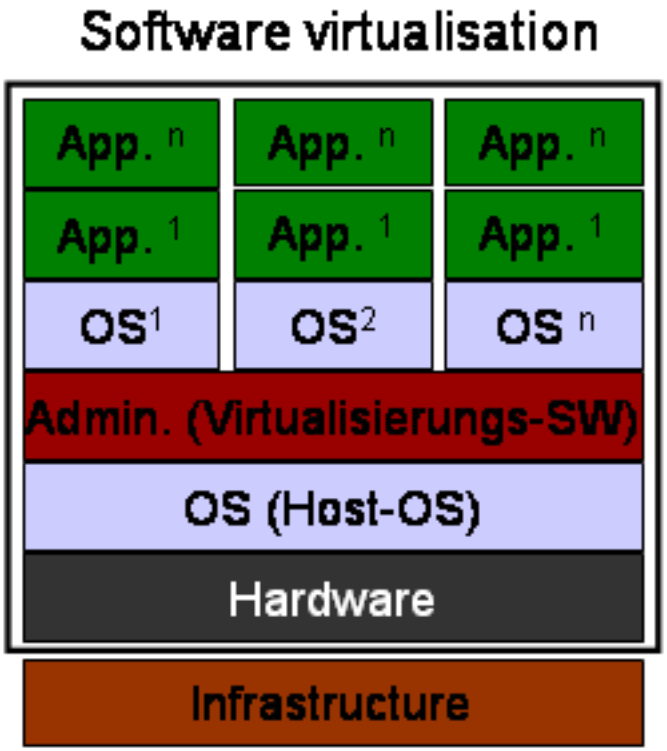
- The administration and control interface makes a separation in different partitions possible

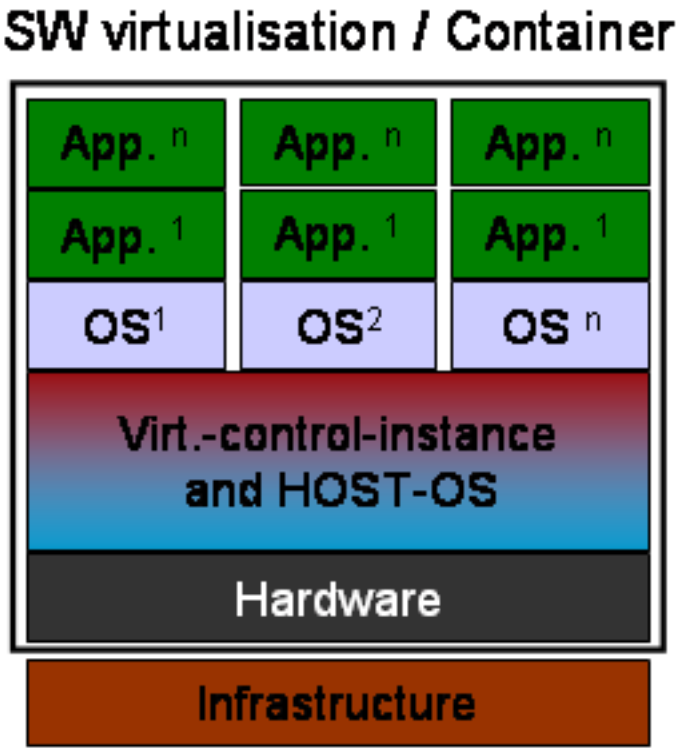




Short Intro to Virtualisation III

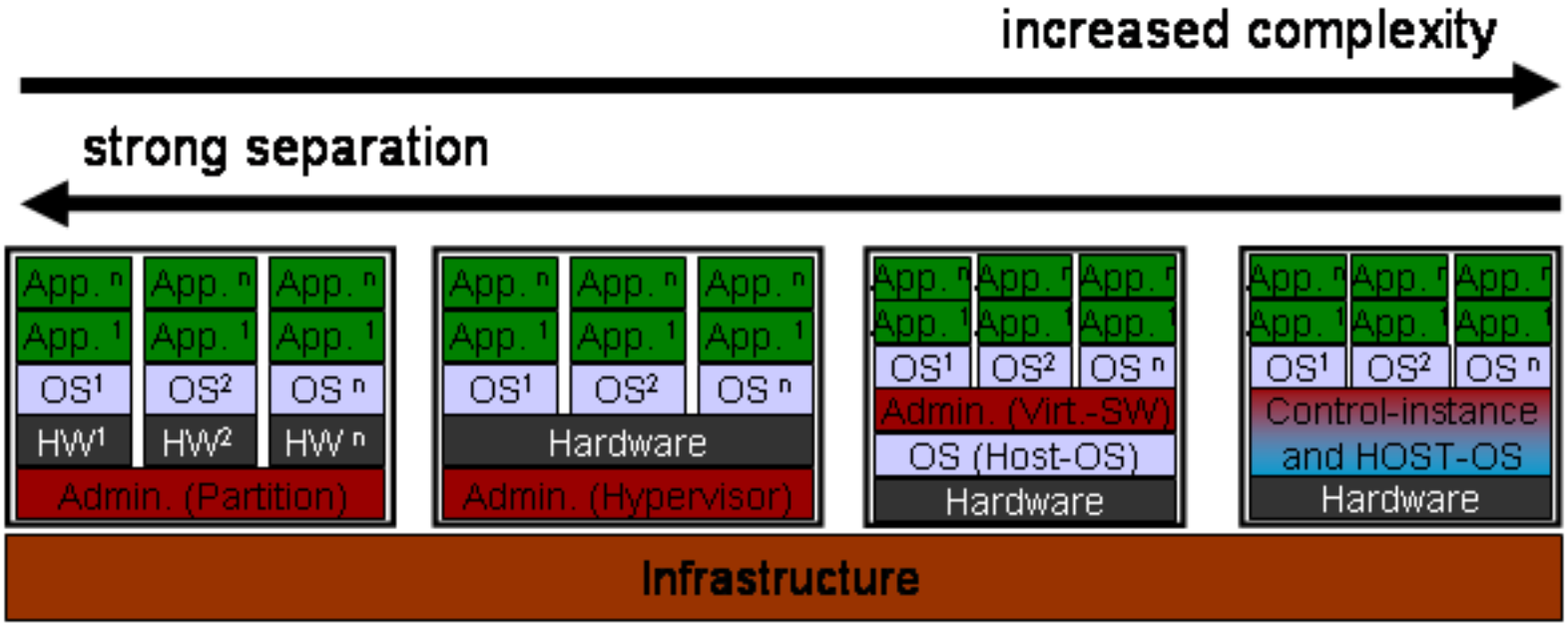
- Within the software virtualisation the administration interface is tied to the operation system





Short Intro to Virtualisation IV

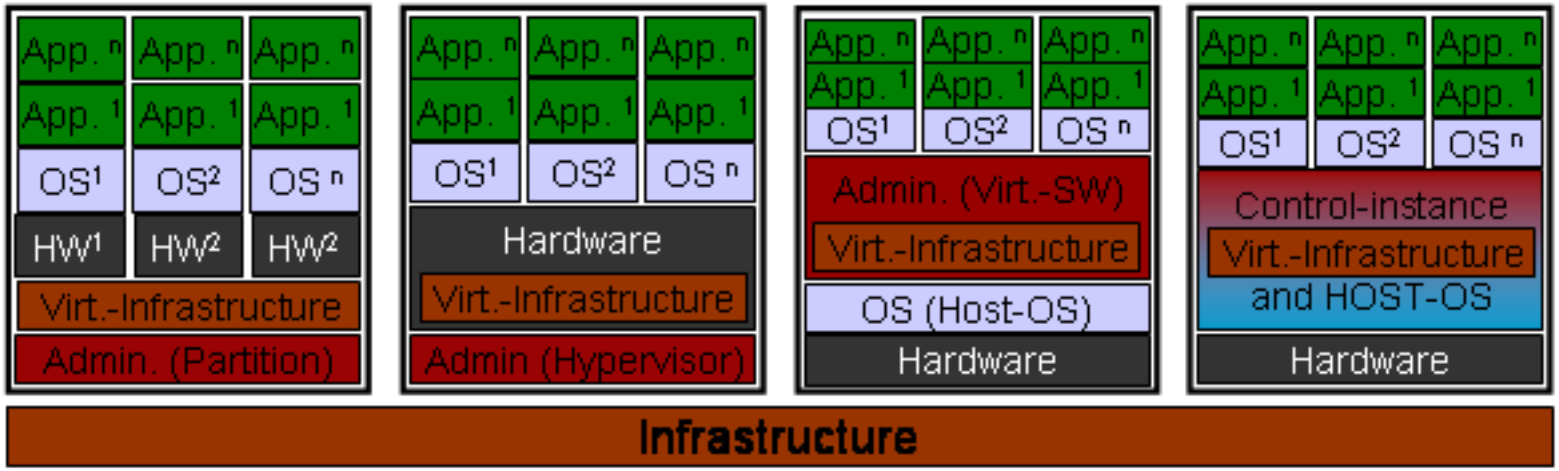
- Functional and security goals stand vis-à-vis
- It is necessary to define uniform standards and regulations for the use of software virtualisation in production



Short Intro to Virtualisation V

- Virtual infrastructure

  Meanwhile, different rudiments to handle server-internal communication exist:
  - virtual switches and router
  - virtual backbones / backplanes and internal networks
  - virtual firewalls / perimeter security



Facts & Threats I

- Virtualisation requires expanded IT-security concepts and IT-system architecture and should be revised
- Compared to non-virtualised systems virtualised systems need to be in the same security condition
- Threats of virtualised systems are more than regular attack pattern for non-virtualised systems …

… an excerpt of possible upcoming threats:

Facts & Threats II

- Compromising of unprotected and unpatched systems and applications via network
- Black box testing, fuzzy analysis, hacking the software
- Unauthorised, undesirable and uncontrolled communication and information leakage (keyword: ‚covert channel‘)
- Resource theft and absorption by other applications
- Bypassing of perimeter security and virus protection
- Partly or fully compromising the host-system or the administration mechanisms and principles
- False implementation or configuration
  (also influenced by increasing complexity)
- „Bottleneck“ within I/O and network (factor to plan!)
- Virtualisation as attack technique:

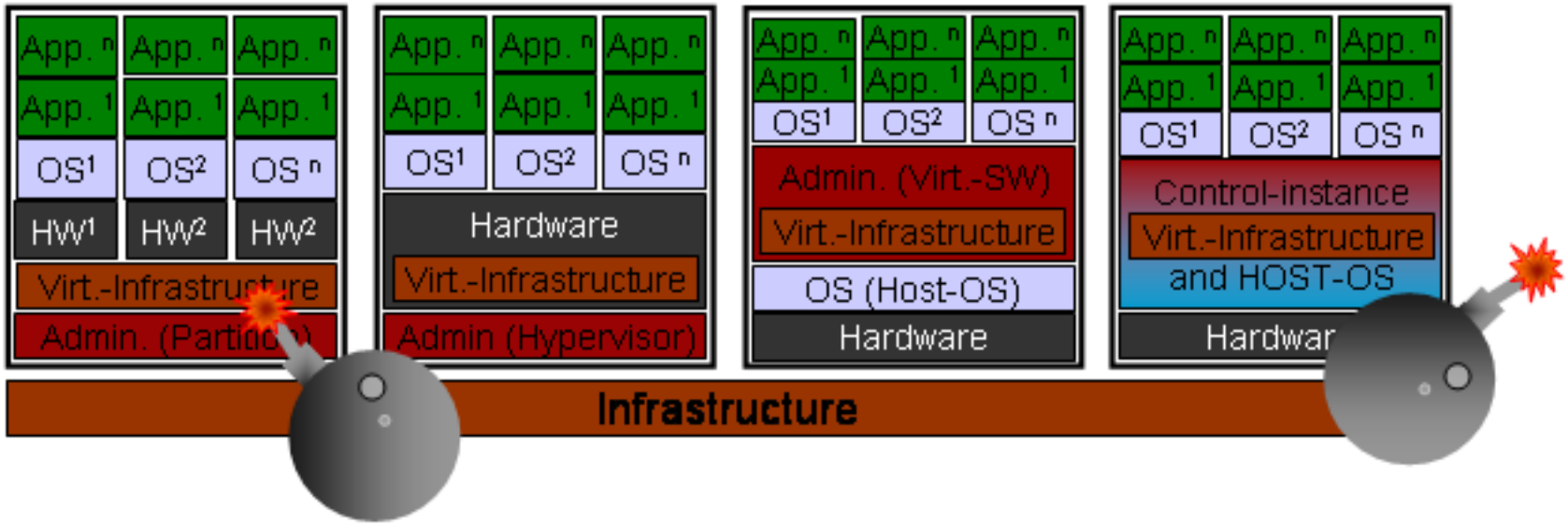
  „Blue-Pill“-attack: VM-rootkit on AMD’s SVM/Pacifica
  „Vitriol“-attack: VM-rootkits on Intel’s VT-x/Vanderpool.

Facts & Threats III

- Virtualisation as a security panacea?

  No!

  Security concepts must be created & revised and measures must be designed & implemented!



Top 1 – Define Standards

- Virtualised and non-virtualised systems must fulfil the same security standards
- No ‘special treatments’ for virtualised systems
- Software, images and processes for installation and operation must be fully comparable to non-virtualised systems
- Proofs, checks, rules and audits must be the same as with non-virtualised systems

Top 2 – Harden, Patch, Update

- Same procedures as with non-virtualised systems
- Base / host-system including virtualised application has to be hardened and the services need to be reduced strongly
- Not-used virtualised services (e.g. virtual switches, router, firewall) need to be deactivated or deinstalled
- Use Hereditary patching
  (every system on the same version)
- Patching & updating is still very important to be prepared against actual vulnerabilities and to reduce risks

Top 3 – Realise Least Privileges

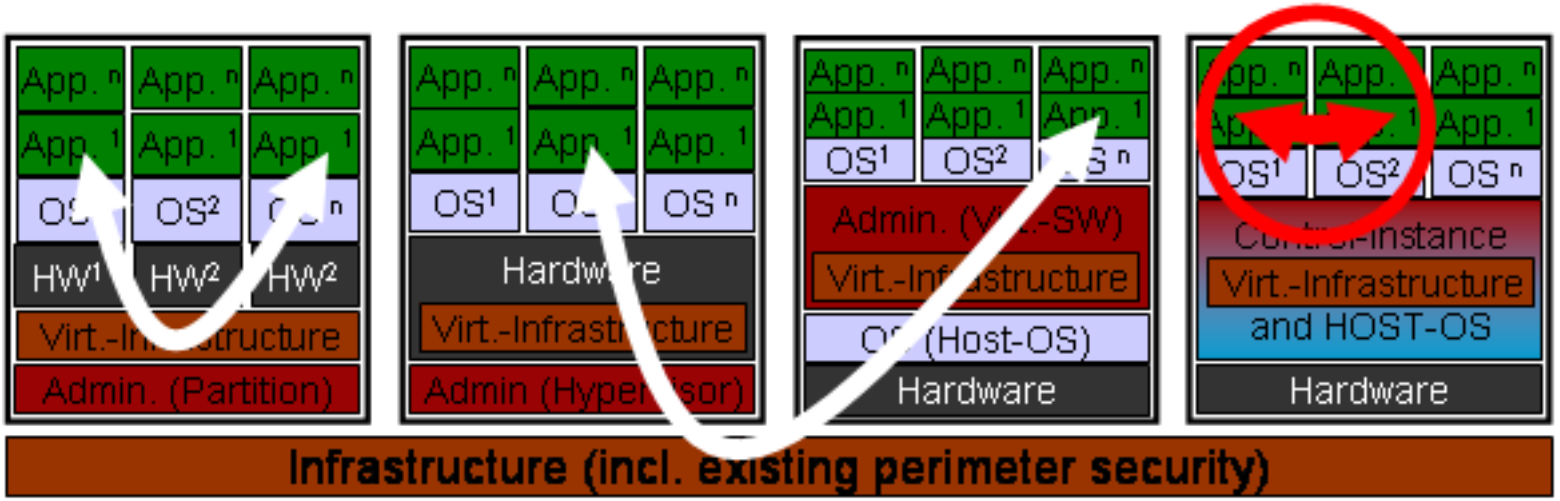
- Realise the principle of least privileges for application, administration and users
- Implement minimization, privilege separation and need-to-know
- Separate your data und isolate them
- Control access to data
- Amongst other, the applied principles reduce unauthorised und undesirable access to data (covert channel)

Top 4 – Control the Connectivity I

- The communication within virtualised systems as well as towards the other infrastructure must be controlled
  - Including network-access-points and installed backplanes
  - The control can be realised via perimeter security
  - Single virtualised applications can also be separated and controlled via perimeter security
- Applications have to be separated and isolated
  - Kernel- and driver hacks are existing for multiple operating systems
  - Hopping attack (encroachment) is possible because of attackable applications

Top 4 – Control the Connectivity II

- The infrastructure, implemented perimeter security and well-defined configurations reduce the communication
- Use perimeter security, for example local firewalls or IP-filter, until security is not an integral part of the system

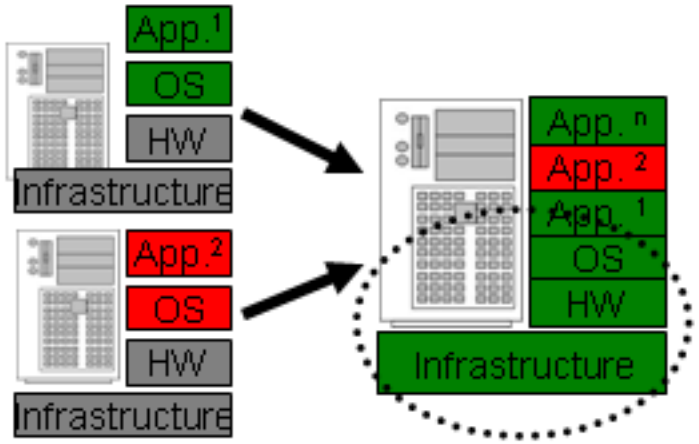


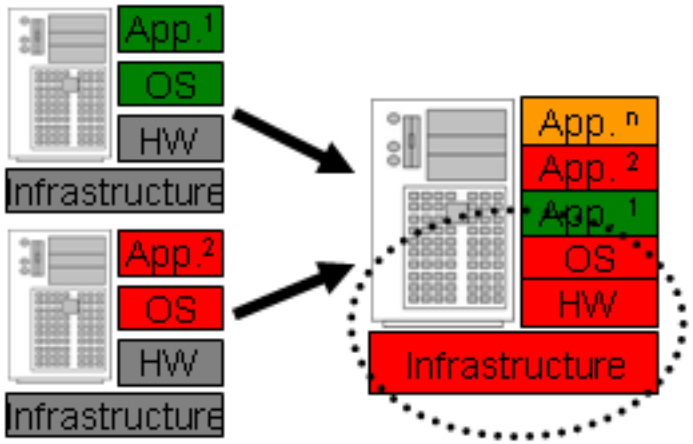
Top 5 – Set up Security-Domains I

- Use security labels
  (security levels and protection requirements need to be defined)
- Define different security domains and zones
- Systems with different security labels must operate at the highest common security standard
- Virtualised and non-virtualised systems must be classified into the security levels
- Different security levels belong to separate security zones and will not be mixed up
  (comparable to ‚mandatory access control‘)

Top 5 – Set up Security-Domains II

- Different security needs must be taken into consideration!
- In certain situations the security standard of the host-system has to be increased
- The weakest link in the chain counts!





Top 6 – Network Separation

- Network separation has to be realised similar to the security zones
- Existing perimeter security (or other security mechanisms) must not be bridged
- Be careful with systems which were separated prior to virtualisation!

Top 7 – Protection against Malware

- Virus-, content- and malicious-code-scanning is also obligatory for virtualised systems
- Implement measures to prevent the breakout from one cell to another
  - Additional: Control the communication and implement the principle of least privilege

Top 8 – Define Resource-Sharing

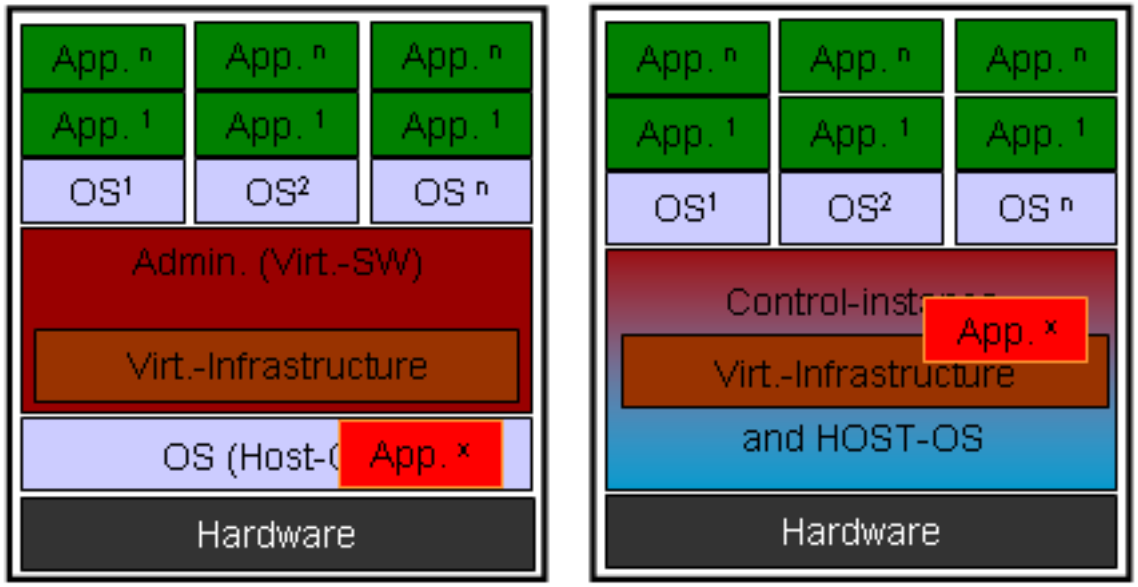
- Resources of the host-systems have to be defined clearly
- Compared to dynamic resource definitions static resource definitions offer an increase of security and improve the resource manageability
  - Memory allocation denial of service within the host-system
  - DoS because of high CPU-load
  - DoS because of ‘classic’ buffer overflows
  - Bridging and resource encroachment of information from one virtual cell / application to another

Top 9 – Protection of Administration

- Protect the administration console and its access
- Protect the configuration files of the host-systems (access, manipulation and integrity)
- The role and access controls have to distinguish and separate administration of host & application (technical)
- Separate roles for host / base-system administration and application administrators (organisational)
- The usage of all administration tools including the change of the hosts-systems parameters (& parameters of virtualisation) must be logged

Top 10 – No Application in the Base

- Applications and services which are about to be virtualised must not be installed on the host-system base
- Standard services and tools within the host-system can also be compromised by flaws and exploits



The Security Concept

- Implement the Top 10 – measures
- Define concrete requirements and definitions of architecture before talking to the vendors
- Analyse the communication relationship as well as the IT-architecture
- Use centralised user & role management
- No guests and users within the protected mode
- No user within the hosts-system base
- Protect the server & install-images (update of offline-VMs)
- No network broadcast! Use controlled instead uncontrolled and targeted communication
- Security measures as an integral part of the virtualisation solution
- Put application and virtualisation machine always in ring 3 (CPU/OS-privilege-security-model)
- Continuous validation and verification of the security measures

Conclusion

- Virtualisation contains risks which have to be identified and need to be reduced with concrete measures
- A compelling security concept will reduce risks – even within latest technologies like virtualisation
- Architecture concepts in an early phase offer a higher benefit and a better integration into the given IT-landscape and will protect the existing infrastructure

Thank you for your attention!

References, Information, Contact

- An empirical study into the security exposure to hosts of hostile virtualized environments, Q1/2007,Tavis Ormandy
- M 2.392 Sicherer Einsatz virtueller IT-Systeme,
  BSI Grundschutzhandbuch, BSI
- VMWare & Virtualisierung; Segen oder eher Fluch für unsere IT-Sicherheit?,
  April 2007, Michael Lüders, LWP GmbH
- Virtualisierung erfordert neue Konzepte in der IT-Security, April 2007,
  Dr. Wilfried Schmitz, SHE AG
- Gartner
- Vendor- or Productinformation
- Securing a virtualised environment, Steve Gold, Aug 2007,
  www.ComputerWeekly.com

Contact:

frank . ackermann -+at+- postbank . de

virtualised . hedge -+at+- web . de