Virtualisation + Security

Today’s Plan

- **9:00 – 9:30: Virtualisation Security (Various Sources).**
- **9:30 – 10:00: Course Review.**
- 10:00 – 12:00 Coursework.

Security Issues

Security Violations

- Five most typical security violations:
  - **Breach of confidentiality:** Unauthorised reading of data (e.g. identity information, credit card numbers, etc.).
  - **Breach of integrity:** Unauthorised modification of data (e.g. modification of the source code of an important commercial application).
  - **Breach of availability:** Unauthorised destruction of data (e.g. website defacement).
  - **Theft of service:** Unauthorised use of resources (e.g. installing unauthorised software).
  - **Denial of service:** Preventing legitimate use of the system (e.g. worms).

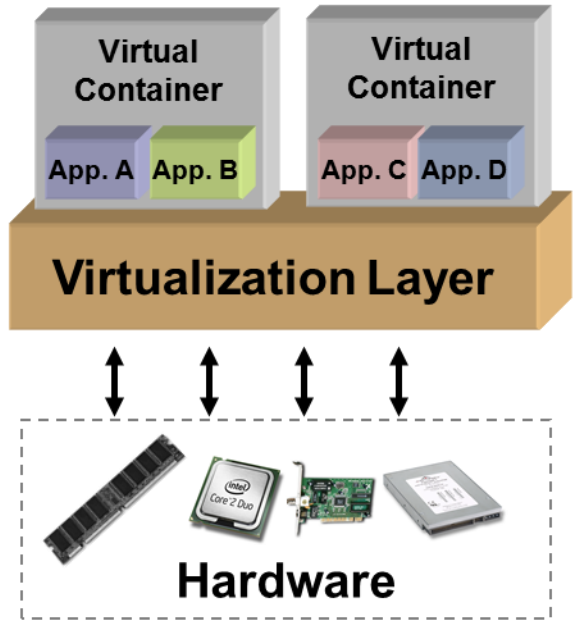
Levels of Impact for Organisations

- **Low:** An anonymous online poll used by a news organisation for subscribers and random users.
- **Medium:** A Moodle-type website that offers a forum facility to the students undertaking a particular module.
- **High:** A hospital patients' medical record system.

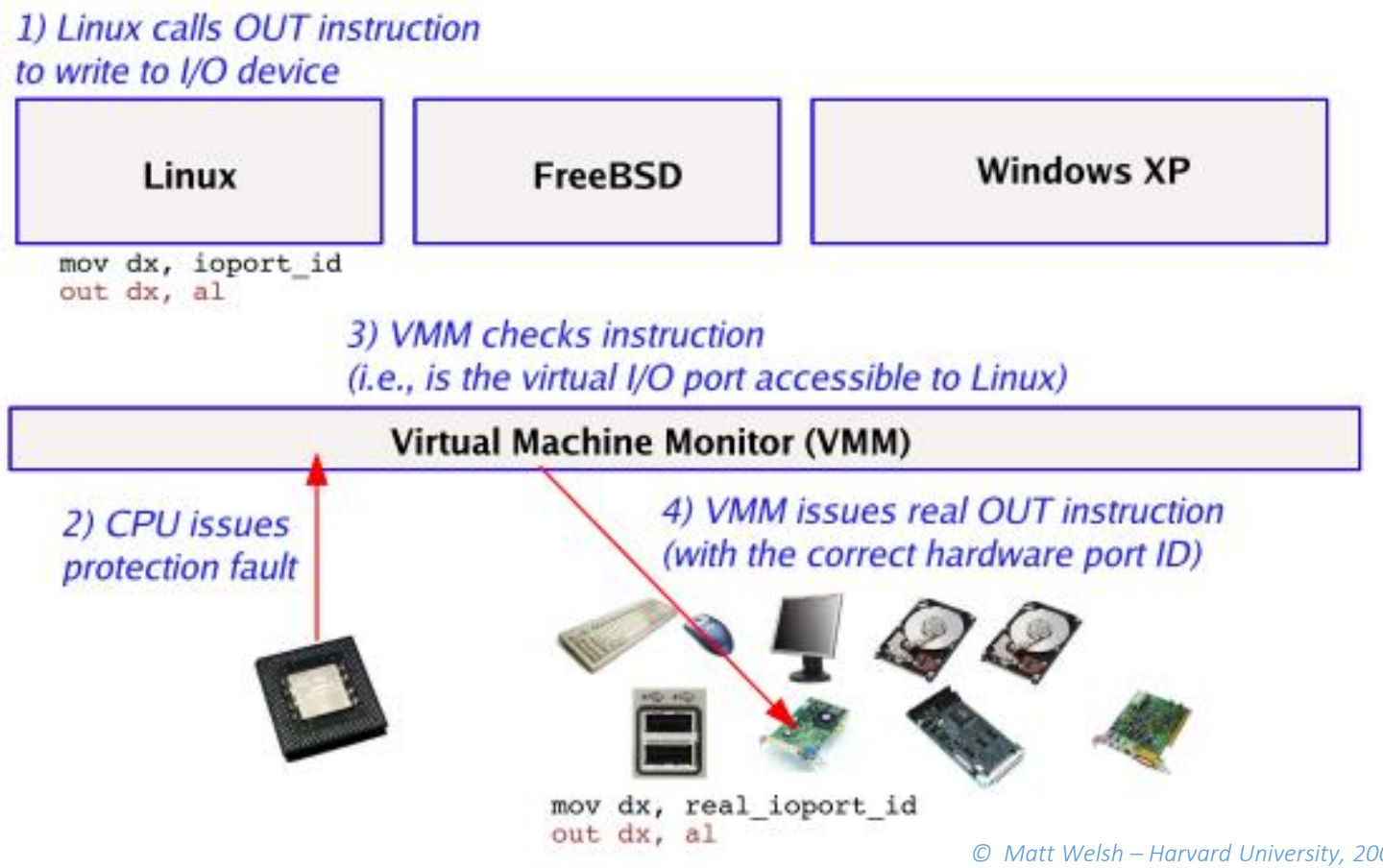
Virtualisation Recap

Virtualisation Recap

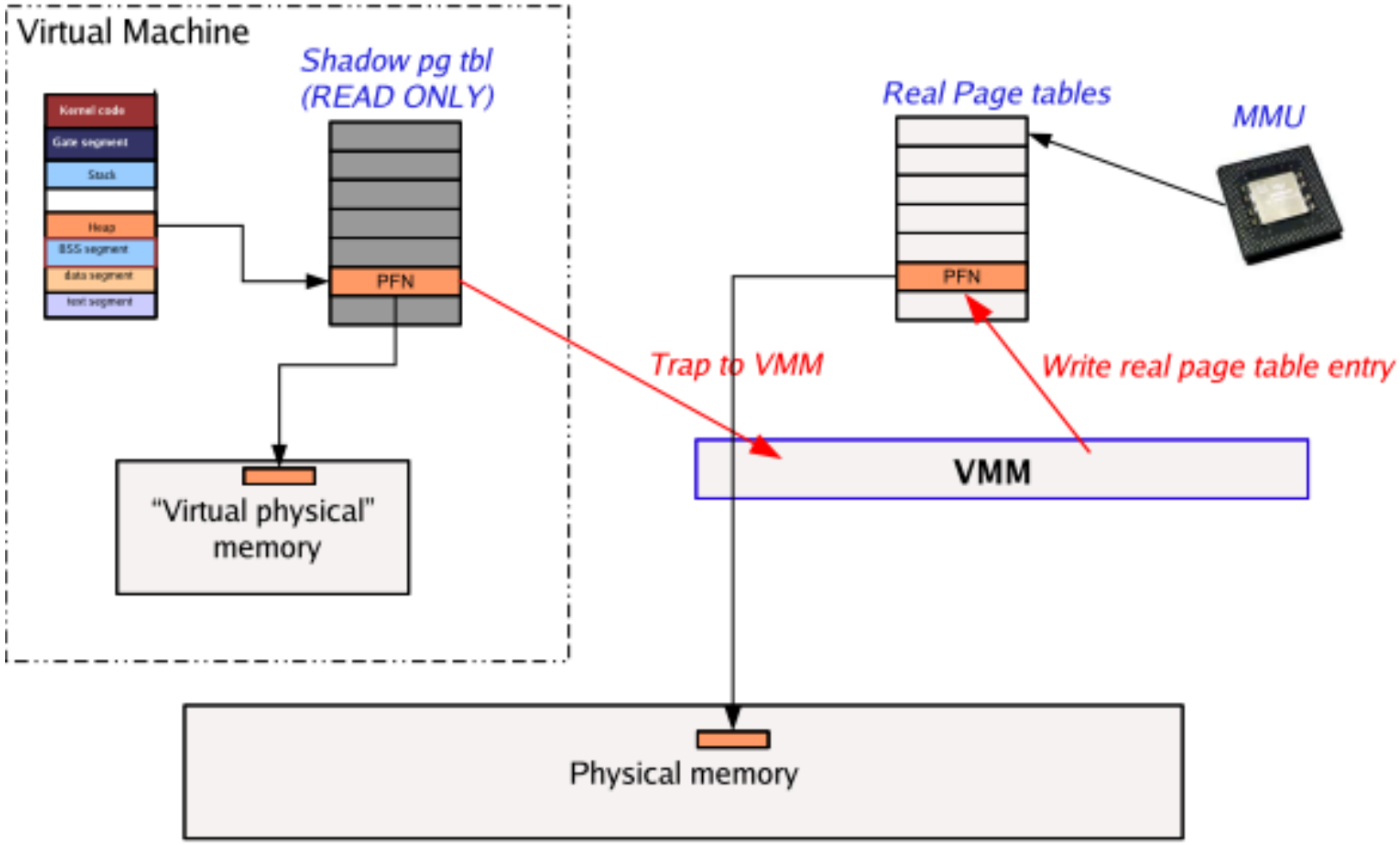
- Creation of a layer that maps the interface of a system (virtual machine) or component (i.e., I/O device) onto the interface and resources of an underlying (possibly different) real system.
- Purposes:
  - Abstraction
  - Replication
  - Isolation
  - Cross compatibility/Encapsulation
- Does not necessarily aim to simplify or hide details.
- Managed by a virtual machine monitor (VMM).



VMM Trap

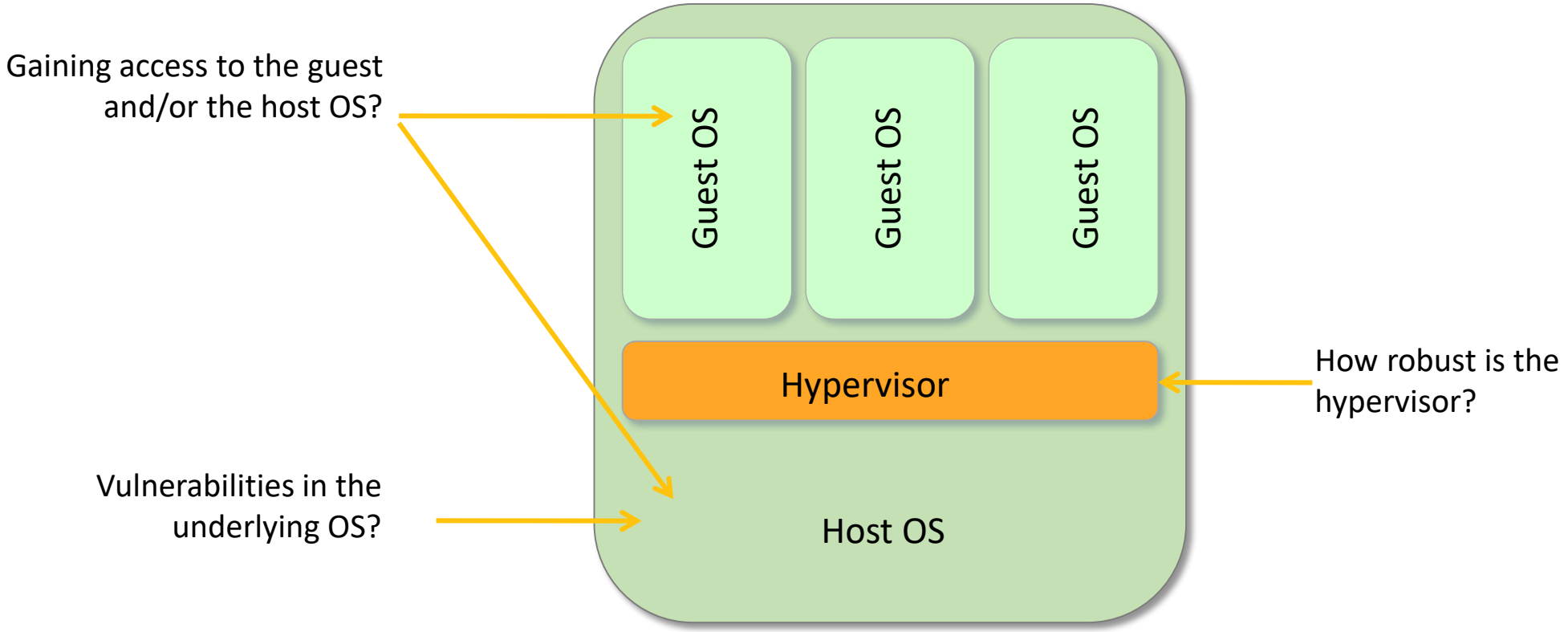


Virtualisation of Memory



Vulnerabilities of VM

Vulnerabilities of Virtualisation



Virtualisation Security Issues

- Hypervisor is the **underlying component** of all these architectures. It is a new layer which needs to be protected!
- **Scale of deployments**:
  - e.g. 150 virtual machines running a simultaneous scheduled anti-virus (AV) scan on the same physical host.
- **Isolation**: Machines of a company and its competitor could be running on the same physical machine.
  - Insufficient isolation could lead to attacks.
- Guest OS monitoring by the hypervisor, which has **privileged access rights**.
- New APIs to access virtualization services:
  - Bugs in these could lead to compromise of entire infrastructure.

Source: Huzur Saran– IIT Delhi, 2009

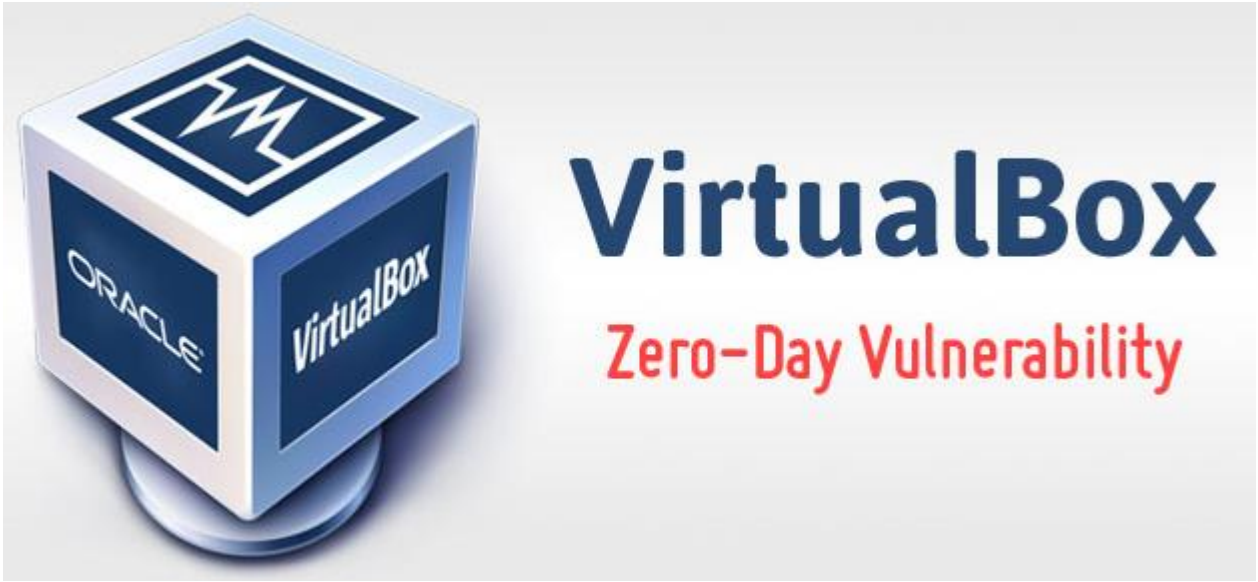
Operational Security Issues

- Most security issues arise not from the virtualisation infrastructure itself but from **operational issues**.
- Adapting existing security processes and solutions to work in the virtualised environment.
- Most security solutions do not care whether a machine is physical or virtual.
- The risk of misconfiguration requires use of **best practices** specific to virtualisation.
  - VMWare.
  - Erick Halter (co-author of *Virtualization: From the desktop to the enterprise).*

Sources: Huzur Saran– IIT Delhi, 2009
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/partners/intel/vmware-intel-best-practices-white-paper.pdf
https://searchservervirtualization.techtarget.com/tip/Best-practices-for-getting-started-with-virtualization

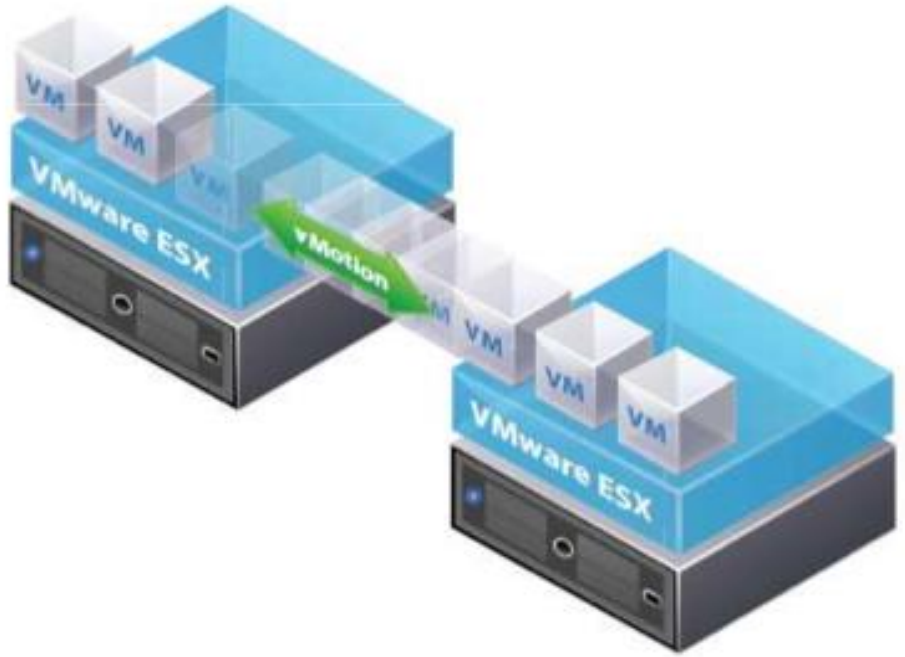
Unpatched VirtualBox Zero-Day Vulnerability

- Allow malware to escape VM and execute code on host OS.
- Occurs due to memory corruption issues on Intel PRO / 1000 MT Desktop (82540EM) network card (E1000) when the network mode is set to NAT.
- DEMO
- How to protect: No patch yet available!
- Change the network card of the VM to PCnet or to Paravirtualised Network.



Source: https://thehackernews.com/2018/11/virtualbox-zero-day-exploit.html

VM Migration



© VMWare Vmotion brochure

- Transfer from one physical server to another with little or no downtime:
  - For load balancing and high availability.
- If transfer is unencrypted, *man-in-the-middle* attack is possible, allowing changes to the VM *enroute*.

Defending Virtualised Systems

Principles and Best Practices

- **Open design**: You need all the help you can get.
- **Economy of mechanism**: Fewer things to get right.
- **Minimize secrets**: Secrets do not remain secret.
- **Fail-safe defaults**: Most users won't change them.
- **Least privilege**: Limit the damage of an accident.
- **Separation of privilege**: Dangerous operation should require multiple principles.
- **Complete mediation**: Check every operation.

Defence-in-depth?

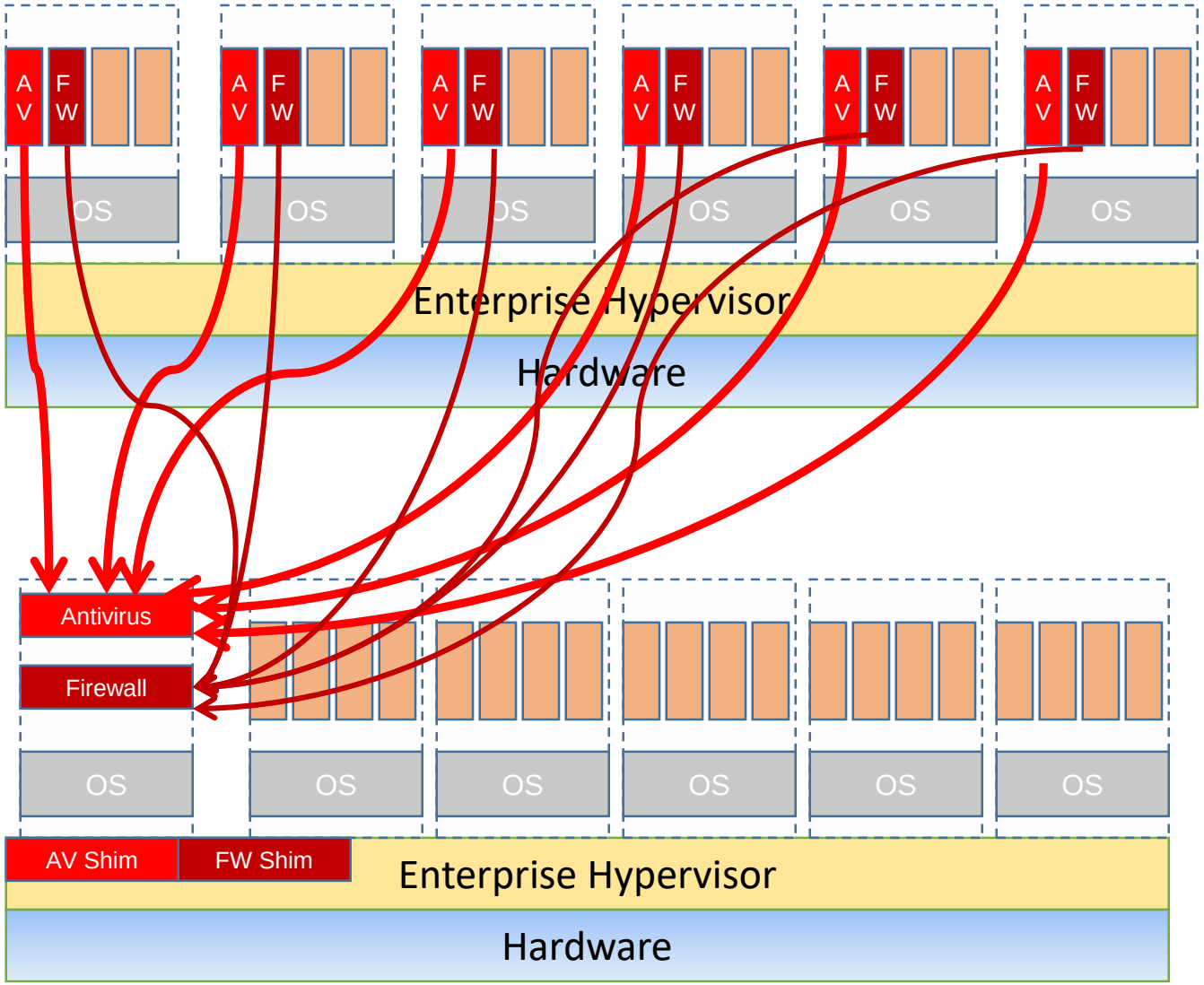
Source: Huzur Saran– IIT Delhi, 2009

Hypervisor Security

- Hypervisors are written by humans:
  - They have bugs, typically buffer overflows.
- Hypervisor are complex:
  - Xen is about 300K source lines of code!
- Should be installed in isolated environment and updated to the latest path level:
  - The same approaches as to OS security.
- Complete isolation is hard:
  - Most systems do not have input–output memory management unit (IOMMU) which make it possible to enable direct memory access (DMA) to arbitrary physical memory.
- Access to hypervisor should be limited to authorised administrators only.
- Use trusted hypervisors.
- Use hypervisor malware security:
  - Hyperguard (Phoenix Technologies): Hypervisor integrity scanner.
  - Deepwatch (Intel Project): Virtualisation rootkit scanner.

Source: Huzur Saran– IIT Delhi, 2009

Dedicated VM Security



Is it a good idea?

Source: Huzur Saran– IIT Delhi, 2009

Security Advantages of Virtualisation

- **Better forensics:**
  - A compromised machine can be **cloned in it current compromised state for forensic analysis.**
- **Faster recovery after an attack:**
  - Once cloned, the **VM can be immediately restored to a known good snapshot** which is much faster than a physical server, reducing the impact of a security-related event.
- **Safe Patching:**
  - You can **quickly revert to a previous state if a patch is unsuccessful**, making you more likely to install security patches sooner.
  - You can create a clone of a production server easily, making you **more likely to test security patches** and more likely to install security patches.
- **More Effective Patching:**
  - VMware Update Manager allows patch scanning and compliance reporting, along with **patch remediation for both online and offline VMs.**
- **More Cost Effective Security Devices.**
  - You can put in place cost effective intrusion detection, vulnerability scanning, and other security related appliances which become global for all virtual environments.
- **Security Abstraction**
  - Provide protection from outside the OS, from a trusted context.
  - View all interactions in such context.

Security Disadvantages of Virtualisation

- Single point of failure.
- Trusted hypervisor.
- Trusted secure context outside the OS of the VM.
- Amount of memory required to store VM images.
- Amount of memory required to store VM snapshots.

Course Review

Week 1: Virtualisation

- Definition
- Pro’s and con’s
- Types
  - Type I
  - Type II
  - Type Hybrid
- Abstraction vs Virtualisation
- Techniques to Virtualise the x86 architecture
  - Full
  - Para-virtualisation/OS assisted
  - Hardware assisted
- Relation between types and techniques
- Other uses of virtualisation
  - Memory virtualisation
  - Application virtualisation
  - Virtual machines

Week 2-3: The Security Landscape and Controlling Computers

- Security Landscape
  - Rule-based
  - Relativistic-based
  - Rational
- Security Process
  - Six steps
  - Features-shared
- Program Execution
  - Data & control sections
  - Programs and processes
  - Switching processes
- Buffer overflows & the Morris worm
  - The finger protocol
  - Fighting the worm and aftermath
- Access Control Strategies for Processes
  - Island
  - Vaults
  - Puzzles
  - Patterns
- Principles
  - Open design
  - Chain of Control
- Keeping Processes Separate
  - Hardware separation
  - Software separation
  - Sharing data & access matrix
- Linux shell commands & scripting

Week 4: Managing Files

- Controlling (accessing) files
  - File system
  - File ownership & access rights
  - Directory access rights
- Executable Files
  - Execution access rights
  - Viruses in executable files
- Sharing & Protecting Files
  - Global policies
    - Isolation
    - File-sharing
  - Tailored Policies
    - Privacy
    - Shared reading
    - Shared updating
- Managing Access Rights
  - Access rights matrix
  - Solution 1: By row (file permissions)
    - Permission Flags (Unix)
  - Solution 2: By column (capability-based security)
    - Access Control Lists (Windows)
- Python
  - Pro’s and con’s
  - Data structures

Week 5: Authenticating Users

- Factors
  - Know (passwords)
  - Have (tokens)
  - Are (biometrics)
  - Others?
  - Multi-factor
- Attacks on Authentication (general)
- Passwords
  - Authentication
  - Hashing
    - crypt()
  - Password guessing/cracking
    - How fast?
      - Increasing the search space (fixed/range)
      - Reducing the search space
  - Dictionary attack
    - How fast is it?
      - Fixed length
      - Range of length
- Tokens
  - Pro's and Con's
  - Types
    - Passive
    - Active
  - Challenge response authentication
- Biometrics
  - Accuracy
- Authentication requirements
  - Threats and motivations
    - Weak
    - Strong
    - Extreme

Week 6: Firewalls and Security Protocols

- Firewalls
  - Packet filter
    - TCP ACK Attack
  - Stateful packet filter
  - Application proxy
  - Defence-in-Depth
- Secure Shell (SSH)
  - Diffie-Hellman
  - SSH simplified
  - Attacks on SSH
- Secure Socket Layer (SSL)
  - SSL simplified
  - Attacks on SSL

Week 7: Malware

- Definition
- Types
  - Parasitic
  - Independent
- Propagation Mechanisms
  - Virus
  - Worm
  - Trojan Horse
- Types of Payload
  - Data destruction
  - Data kidnapping
  - Real-world damage
  - Logic bombs
  - Bots/Zombies
  - Information theft (phishing)
  - Stealthing (rootkits)

Week 8: Operating System Security

- Protection vs security
- Access control
- Protection of objects
- OS Hardening
- Trusted computer base
- Security maintenance
- Security threat monitoring

- OS Security case studies
  - Linux
    - Access control
    - Pluggable Authentication Modules
    - Vulnerabilities
  - Windows
    - Facilities
    - User authentication
    - Vulnerabilities

Week 9: Malware and Software Security

- Malware prevention
  - Elements
  - Effective countermeasures
  - Technical mechanisms
  - Places
    - In host
      - Simple scanner
      - Heuristic scanner
      - Activity traps
      - Full-feature protection
        - Generic Decryption
        - Host Based Behaviour Blocking System
        - Spyware detection and removal
        - Rootkit countermeasures
    - In network
      - Ingress monitors
      - Egress monitors
    - In general
      - Distributed Intelligence Gathering

- Software security
  - Intended vs implemented
  - Types of flaws
    - Bugs
    - Trap door
  - Bad software
  - Software insecurity
  - Software security assurance
  - Software security questions
  - Software security examples
  - Software security categories
    - Insecure interaction
    - Risky resource management
    - Porous defences
    - Handling input
  - Software security best practices

Week 10: Virtualisation + Security

- Security Issues
  - Violations
    - Breach of confidentiality
    - Breach of integrity
    - Breach of availability
    - Theft of service
    - Denial of service
  - Level of impacts for organisations
    - Low
    - Medium
    - High
  - Vulnerabilities of a VM
    - Security issues
    - Operational issues
- Defending virtualised systems
  - Principles and best practices
  - Hypervisor security
  - Dedicated VM security
- Virtualisation for security
  - Pro’s and con’s