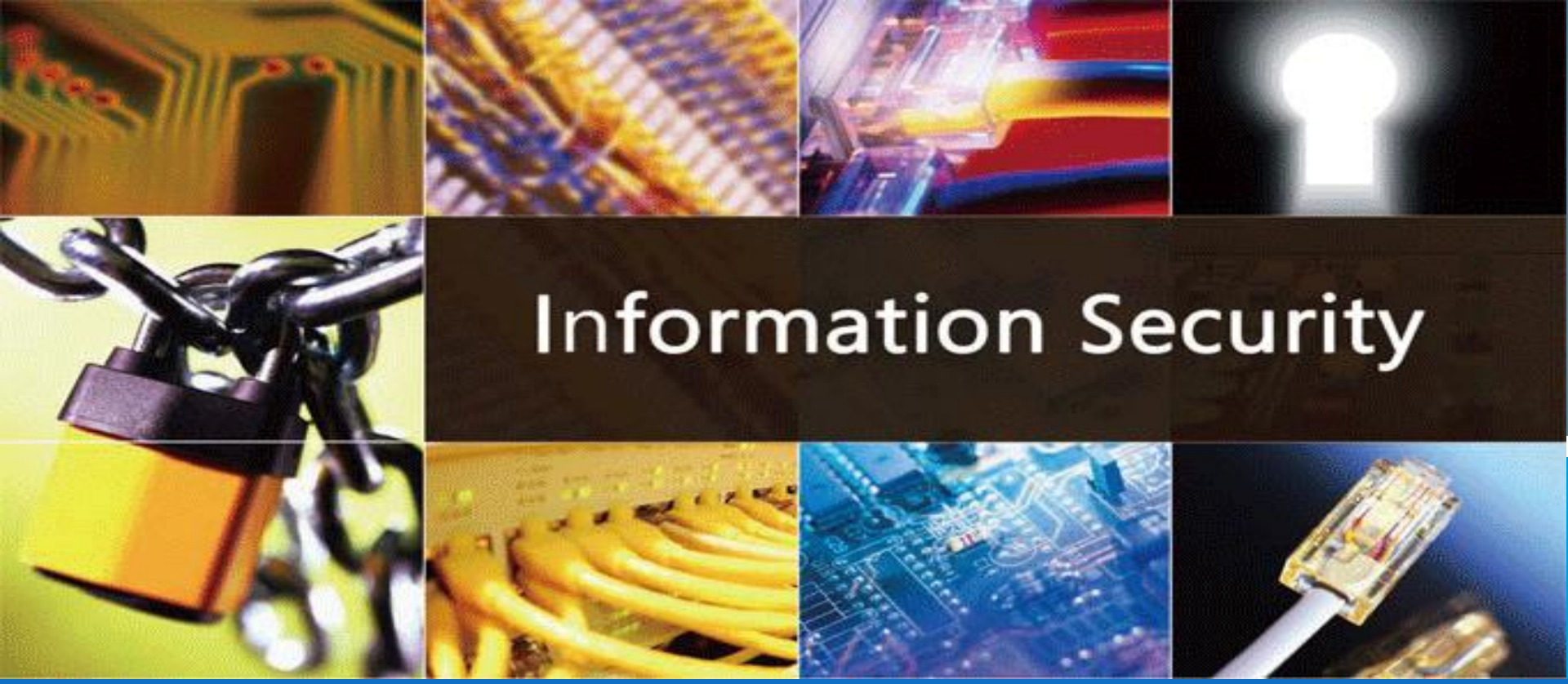


Operating Systems Security

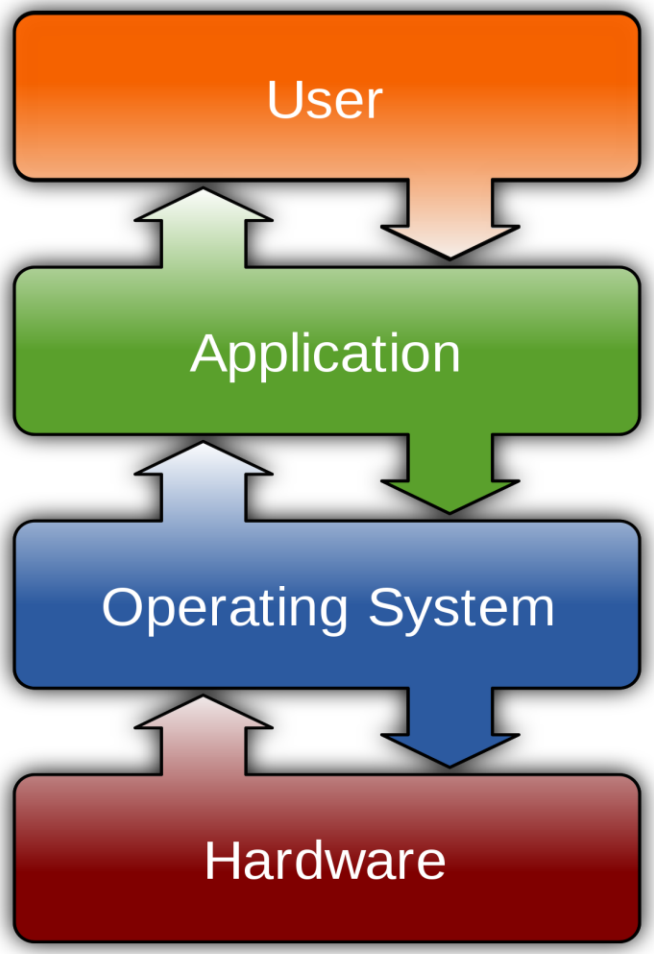
Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Contents

- Introduction To OS and OS Security
- System Security Planning
- The Components of an OS Security Environment
- Vulnerabilities of OS
- Secure an operating system
- Operating Systems Hardening
  - Linux/Unix Security
  - Windows Security
- Virtualization Security

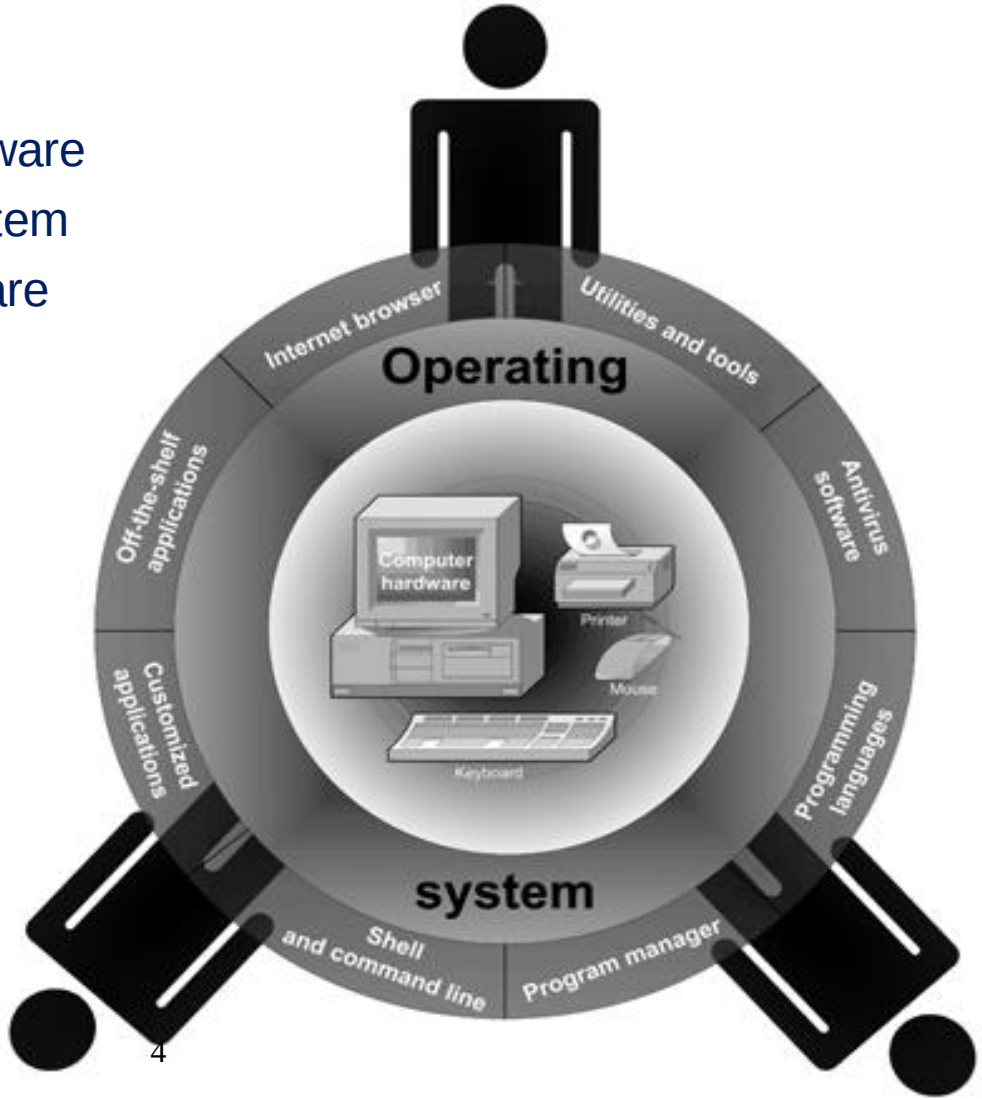
Operating System Overview

- Operating system: collection of programs that allows user to operate computer hardware



Operating System Overview

- Three layers:
  - Inner layer, computer hardware
  - Middle layer, operating system
  - Outer layer, different software



Operating System Overview

- Key functions of an operating system:
  - Multitasking, multisharing
  - Computer resource management
  - Controls the flow of activities
  - Provides a user interface
  - Administers user actions and accounts
  - Runs software utilities and programs
  - Enforce security measures
  - Schedule jobs
  - Provide tools to configure the operating system and hardware

Need for Trusting an Operating System

Why do we need to **trust** the operating system?
(a **trusted computing base or TCB**)
What requirements must it meet to be trusted?

TCB Requirements:

1. Tamper-proof,
2. Complete mediation, and
3. Correct

Trusted Computing Base (TCB)

- Think carefully about what you are trusting with your information
  - if you type your password on a keyboard, you're trusting:
    - the keyboard manufacturer
    - your computer manufacturer
    - your operating system
    - the password library
    - the application that's checking the password
  - TCB = set of components (hardware, software, wetware) that you trust your secrets with
- Public web kiosks should *not* be in your TCB
  - should your OS?
    - but what if it is promiscuous? (e.g., IE and active-X extensions)
  - how about your compiler?
    - A great read: "Reflections on Trusting Trust".

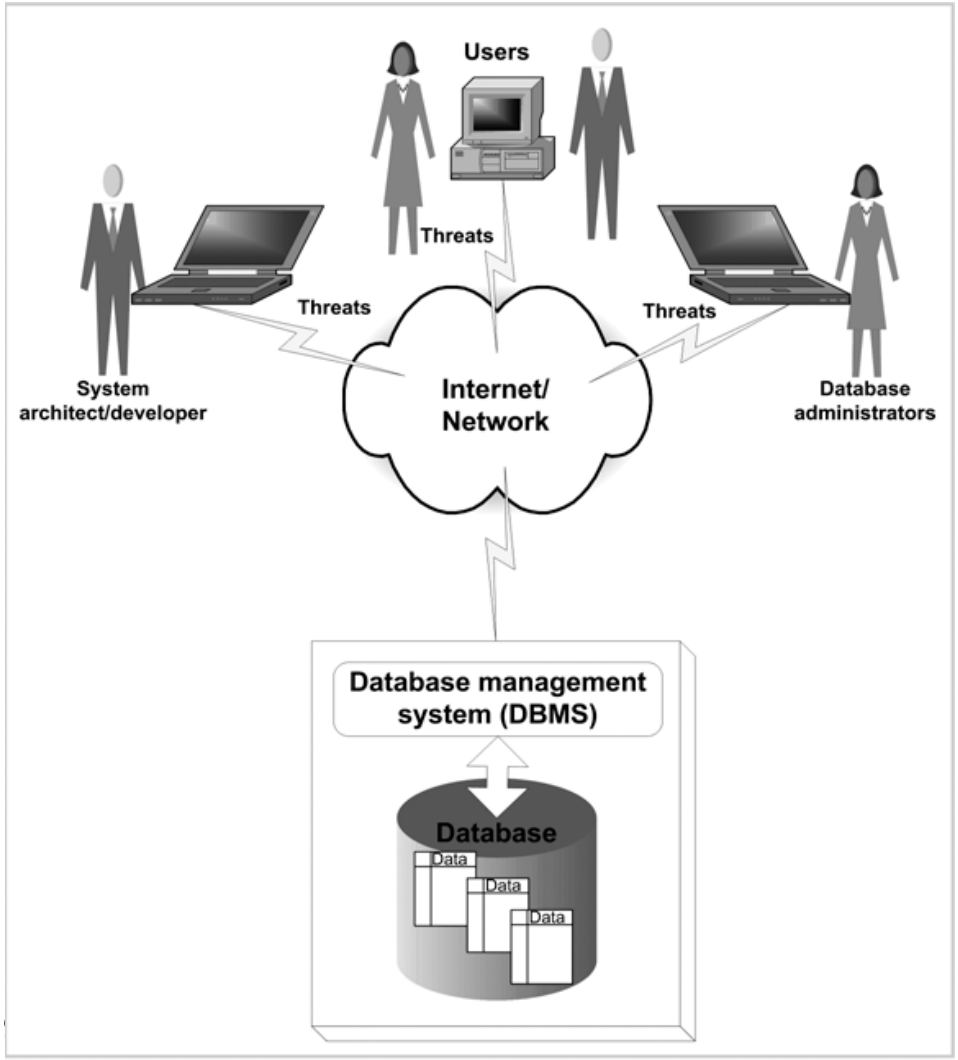
TCB and Resource Protection

TCB Controls access to protected resources

- Must establish the source of a request for a resource (authentication is how we do it)
- Authorization or access control
- Mechanisms that allow various policies to be supported

The OS Security Environment

- A compromised OS can compromise a database environment
- Physically protect the computer running the OS (padlocks, chain locks, guards, cameras)
- Model:
  - Bank building (operating system)
  - Safe (database)
  - Money (data)



The Components of an OS Security Environment

- Used as access points to the database
- Three components:
  - Services
  - Files
  - Memory

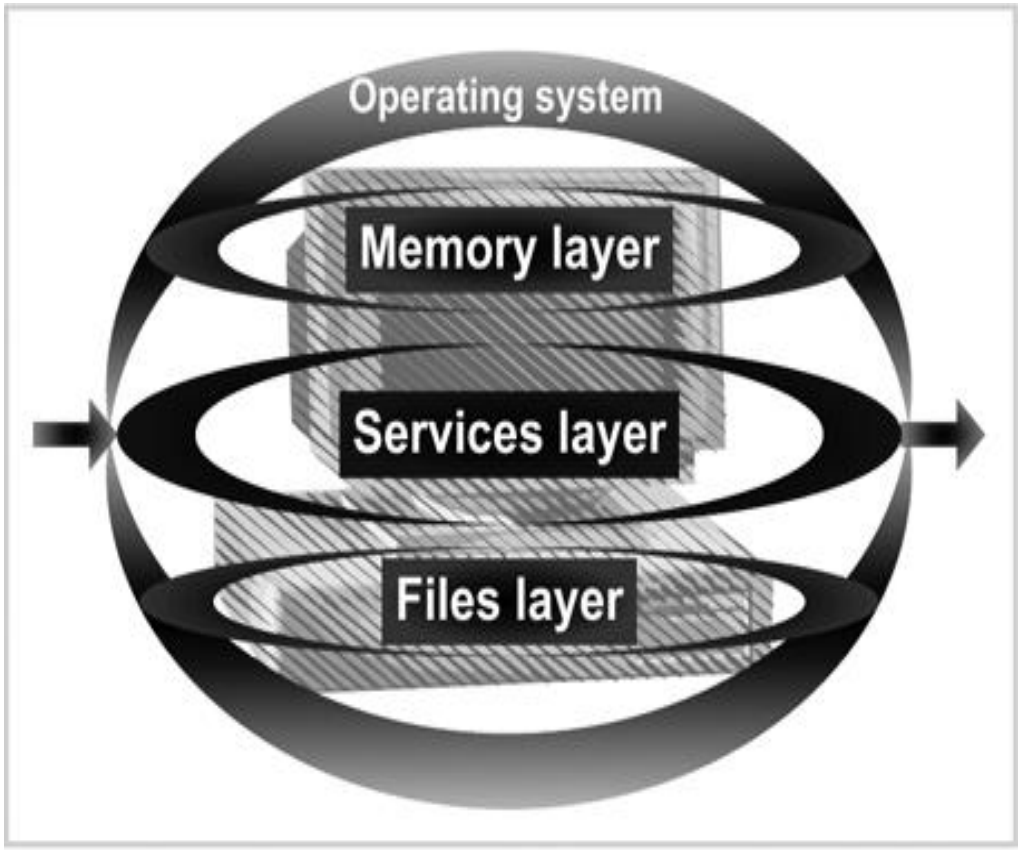


FIGURE 2-3 Operating system security environment

Services

- Main component of operating system security environment
- Used to gain access to the OS and its features
- Include
  - User authentication
  - Remote access
  - Administration tasks
  - Password policies

Files

- Common threats:
  - File permission
  - File sharing
- Files must be protected from unauthorized reading and writing actions
- Data resides in files; protecting files; protects data

File Permissions

- Read, write, and execute privileges
- In Windows:
  - Change permission on the Security tab on a file's Properties dialog box
  - Allow indicates grant; Deny indicates revoke
- In UNIX/Linux
  - Three permission settings: owner; group to which owner belongs; all other users
  - Each setting consist of rwx
    - r for reading, w for writing, and x for executing
  - CHMOD command used to change file permissions

File Permissions (continued)

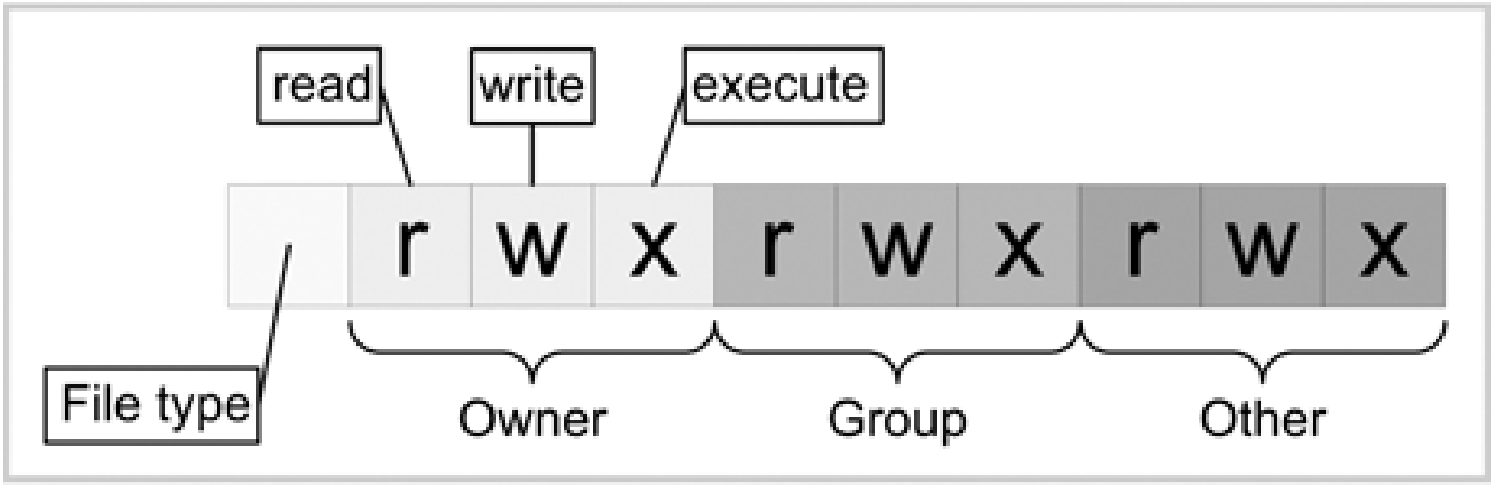


FIGURE 2-5 UNIX file permissions

```
$ chmod  644  mail_list
```

File Transfer

- FTP (File Transfer Protocol):
  - Internet service for transferring files from one computer to another
  - Transmits usernames and passwords in plaintext
  - Root account cannot be used with FTP
  - Anonymous FTP: ability to log on to the FTP server without being authenticated
- Best practices:
  - Use Secure FTP utility if possible
  - Make two FTP directories:
    - One for uploads with write permissions only
    - One for downloads with read permissions only
  - Use specific accounts with limited permissions
  - Log and scan FTP activities
  - Allow only authorized operations

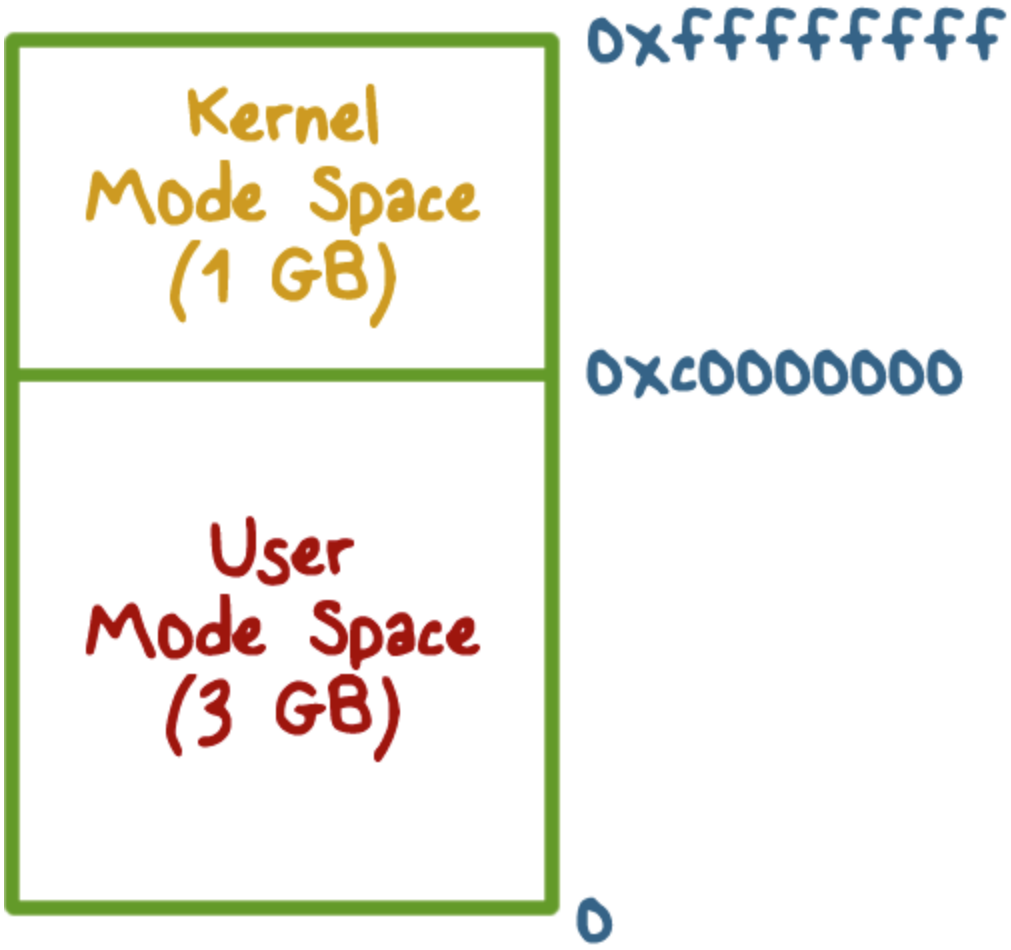
Sharing Files

- Naturally leads to security risks and threats
- Peer-to-peer programs: allow users to share files over the Internet
- Reasons for blocking file sharing:
  - Malicious code
  - Adware and spyware
  - Privacy and confidentiality
  - Pornography
  - Copyright issues

Memory

- Hardware memory available on the system can be corrupted by badly written software
- Can harm data integrity
- Two options:
  - Stop using the program
  - Apply a patch (service pack) to fix it

Linux User/Kernel Memory Split



Authentication Methods

- Authentication: Verifies user access to the operating system
- Physical authentication:
  - Allows physical entrance to company property
  - Magnetic cards and biometric measures
- Digital authentication: verifies user identity by digital means
- Digital certificates: identifies and verifies holder of certificate
- Digital token (security token):
  - Small electronic device
  - Displays a number unique to the token holder;
  - Uses a different password each time
- Digital card: Also known as a security card or smart card
  - Similar to a credit card; uses an electronic circuit instead of a magnetic strip
  - Stores user identification information
- Kerberos:
  - Developed by MIT
  - Uses tickets for authentication purposes

Authentication Methods (continued)

- Lightweight Directory Access Protocol (LDAP):
  - Developed by the University of Michigan
  - A centralized directory database stores:
    - Users (user name and user ID)
    - Passwords
    - Internal telephone directory
    - Security keys
  - Efficient for reading but not suited for frequently changing information
- NT LAN Manager (NTLM):
  - Developed and used by Microsoft
  - Employs a challenge/response authentication protocol
- Public Key Infrastructures (PKI):
  - User keeps a private key
  - Authentication firm holds a public key
  - Encrypt and decrypt data using both keys

Authentication Methods (continued)

- RADIUS: used by network devices to provide a centralized authentication mechanism
- Secure Socket Layer (SSL): authentication information is transmitted over the network in an encrypted form
- Secure Remote Password (SRP):
  - Password is not stored locally
  - Invulnerable to brute force or dictionary attacks

Authorization

- Process that decides whether users are permitted to perform the functions they request
- Authorization is not performed until the user is authenticated
- Deals with privileges and rights

User Administration

- Create user accounts
- Set password policies
- Grant privileges to users
- Best practices:
  - Use a consistent naming convention
  - Always provide a password to an account and force the user to change it at the first logon
  - Protect passwords
  - Do not use default passwords

User Administration (continued)

- Best practices (continued):
  - Create a specific file system for users
  - Educate users on how to select a password
  - Lock non-used accounts
  - Grant privileges on a per host basis
  - Do not grant privileges to all machines
  - Use ssh, scp, and Secure FTP
  - Isolate a system after a compromise
  - Perform random auditing procedures

Password Policies

- First line of defense
- Dictionary attack: permutation of words in dictionary
- Make hard for hackers entering your systems
- Best password policy:
  - Matches your company missions
  - Enforced at all level of the organization

Password Policies (continued)

- Best practices:
  - Password aging
  - Password reuse
  - Password history
  - Password encryption
  - Password storage and protection
  - Password complexity
  - Logon retries
  - Single sign-on enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again

E-mail Security

- Tool must widely used by public
- May be the tool must frequently used by hackers:
  - Viruses; Worms; Spam; Others
- Used to send private and confidential data as well as offensive material
- Used by employees to communicate with:
  - Clients
  - Colleagues
  - Friends
- Recommendations:
  - Do not configure e-mail server on the same machine where sensitive data resides
  - Do not disclose technical details about the e-mail server

Vulnerabilities of OS

- Top vulnerabilities to Windows systems:
  - Internet Information Services (IIS)
  - Microsoft SQL Server (MSSQL)
  - Windows Authentication
  - Internet Explorer (IE)
  - Windows Remote Access Services
  - Microsoft Data Access Components (MDAC)
  - Windows Scripting Host (WSH)
  - Microsoft Outlook and Outlook Express
  - Windows Peer-to-Peer File Sharing (P2P)
  - Simple Network Management Protocol (SNMP)

National Vulnerability Database:

http://nvd.nist.gov/

Vulnerabilities of OS

- Top vulnerabilities to UNIX systems:
  - BIND Domain Name System
  - Remote Procedure Calls (RPC)
  - Apache Web Server
  - General UNIX authentication accounts with no passwords or weak passwords
  - Clear text services
  - Sendmail
  - Simple Network Management Protocol (SNMP)
  - Secure Shell (SSH)
  - Misconfiguration of Enterprise Services NIS/NFS
  - Open Secure Sockets Layer (SSL)

National Vulnerability Database:

http://nvd.nist.gov/

Secure an operating system

- Basic steps
  - Install and patch the operating system.
  - Harden and configure the OS to adequately address the identified security needs of the system by:
    - Removing unnecessary services, applications, and protocols.
    - Configuring users, groups, and permissions.
    - Configuring resource controls.
  - Install and configure additional security controls, such as anti-virus, hostbased firewalls, and IDS, if needed.
  - Test the security of the basic OS to ensure that the steps taken adequately address its security needs.

Operating Systems Hardening

- Hardening:
  - attempting to make OS bulletproof.
  - Ideally - leave OS exposed to the general public on the Internet without any other form of protection.
  - A hardened system should serve only one purpose--it's a Web server or DNS or Exchange server, and nothing else. These systems need too many functions to be properly hardened.

Harden Windows - minimum

- **Disable all unnecessary services.**
  - determine which services can be disabled.
    - Remote Procedure Call (RPC) service.
    - little documentation exists to identify what services a given purpose will require.
    - knowing which services are required and which can be disabled is largely a matter of trial and error.
- **Remove all unnecessary executables and registry entries.**
  - Forgetting to remove unneeded executables and registry entries might allow an attacker to invoke something that had previously been disabled.
- **Apply appropriately restrictive permissions to files, services, end points and registry entries.**
  - Inappropriate permissions could give an attacker an opening.
  - The ability to launch CMD.EXE as "LocalSystem," for example, is a classic backdoor.

Harden Windows for maximum security

- **Adjusting retransmission of SYN-ACKS**. This makes connection responses time out more quickly during a SYN flood.
- **Determining how many times TCP retransmits** an unacknowledged data segment on an existing connection. TCP retransmits data segments until they are acknowledged or until this value expires.
- **Disabling ICMP Router Discovery Protocol** (IRDP) where an attacker may remotely add default route entries on a remote system.
- **Disabling these services**: Telnet, Universal Plug and Play Device Host, IIS, Disable Guest accounts
- **Use the Local Security Policy**
- **Disable File and Print Sharing**.
- **Disable Remote Assistance and Remote Desktop**
- **Use NTFS File system**.
- **Disable auto-logins**.

Harden Linux

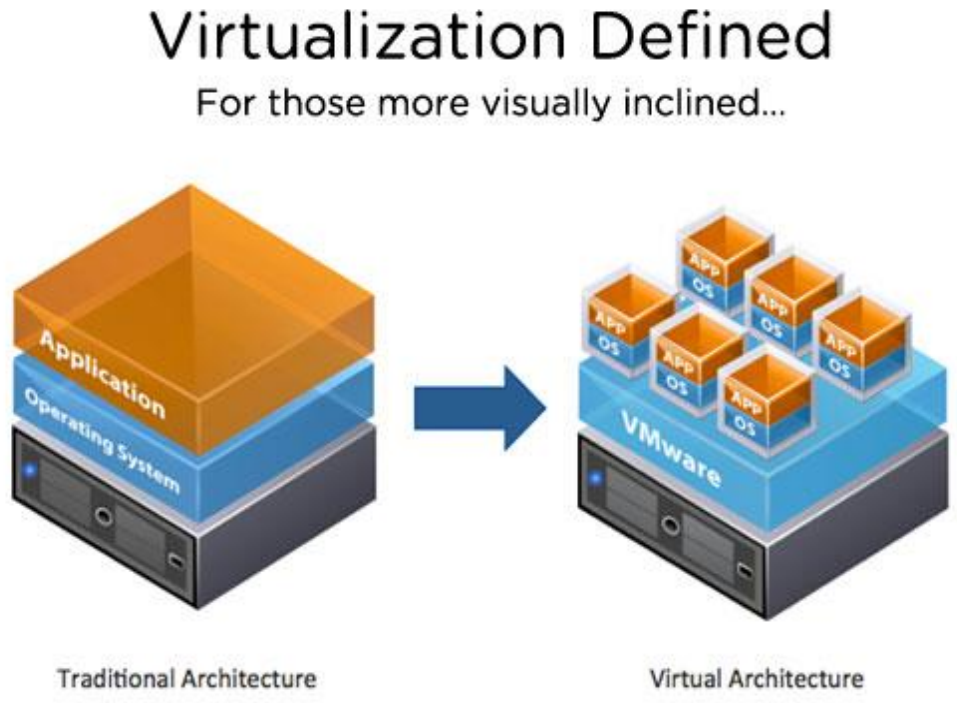
- Encrypt Data Communication
- Avoid Using FTP, Telnet, And Rlogin / Rsh Services
- Minimize Software to Minimize Vulnerability
- One Network Service Per System or VM Instance
- Keep Linux Kernel and Software Up to Date
- Use Linux Security Extensions
- SELinux
- Password: Policy, Aging, Empty
- Login:
  - Locking User Accounts After Login Failures
  - Make Sure No Non-Root Accounts Have UID Set To 0
  - Disable root Login

Harden Linux

- Disable Unwanted Services
- Find Listening Network Ports
- Configure Iptables and TCPWrappers
- Linux Kernel /etc/sysctl.conf Hardening
- Separate Disk Partitions
- Disk Quotas
- Turn Off IPv6
- Disable Unwanted SUID and SGID Binaries
- Logging and Auditing
- Secure OpenSSH Server
- Install And Use Intrusion Detection System
- Disable USB/firewire/thunderbolt devices

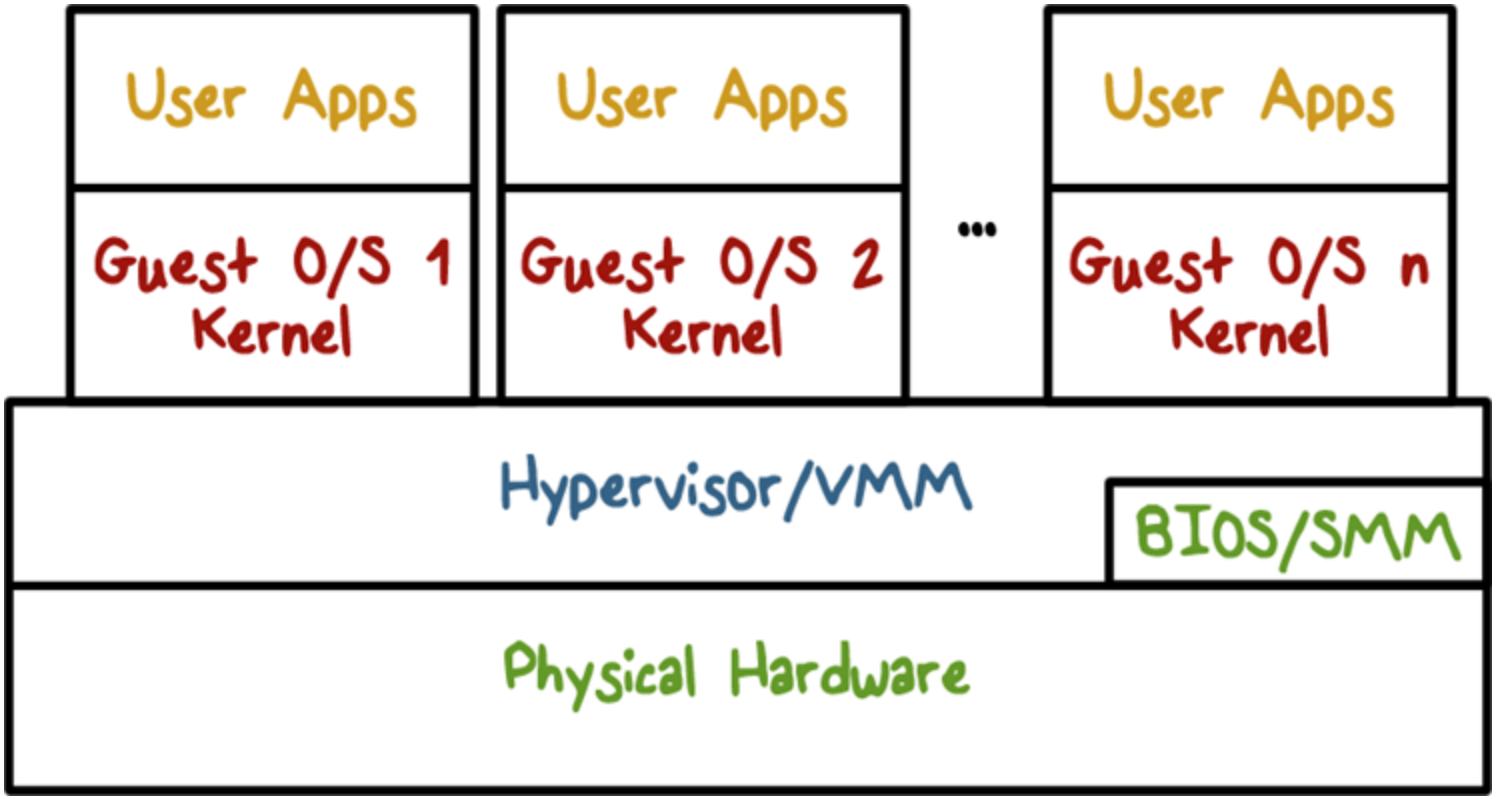
Virtualization Security - Introduction

- A VM is a software implementation of a machine that execute programs like a physical machine
- A VM can support individual processes or a complete system depending on the abstraction level where virtualization occurs.
- Virtualization – a technology that allows running two or more OS side by side on one PC or embedded controller



VM Architecture

•q

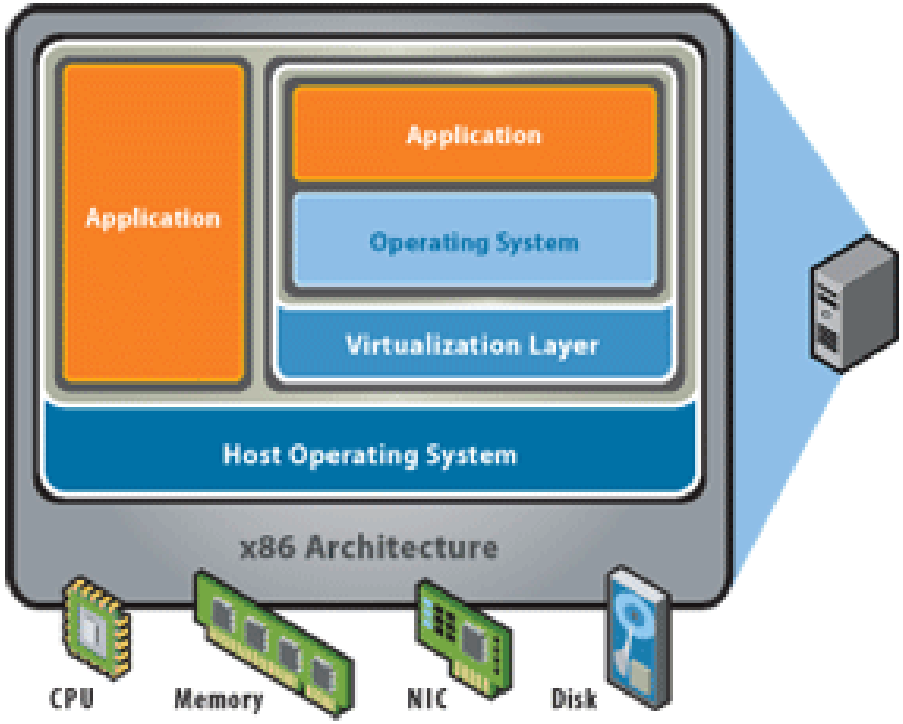


VM Architecture

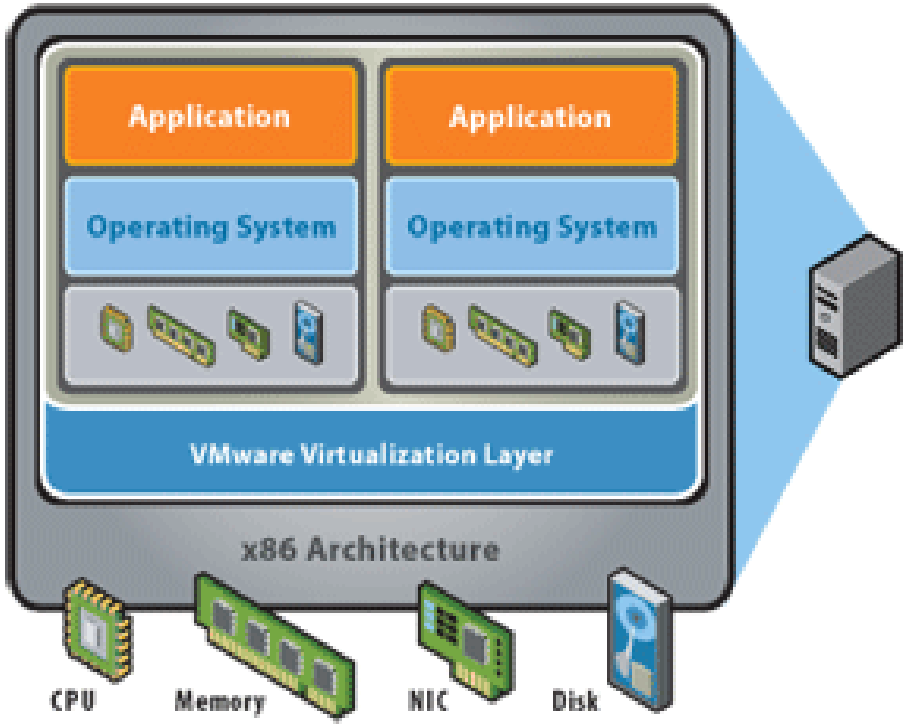
More security implications because of the reliance on the underlying OS, used in VMware and MS Virtual PC

VM is installed that communicates directly with system hardware rather than relying on a host OS

Hosted



Bare - Metal

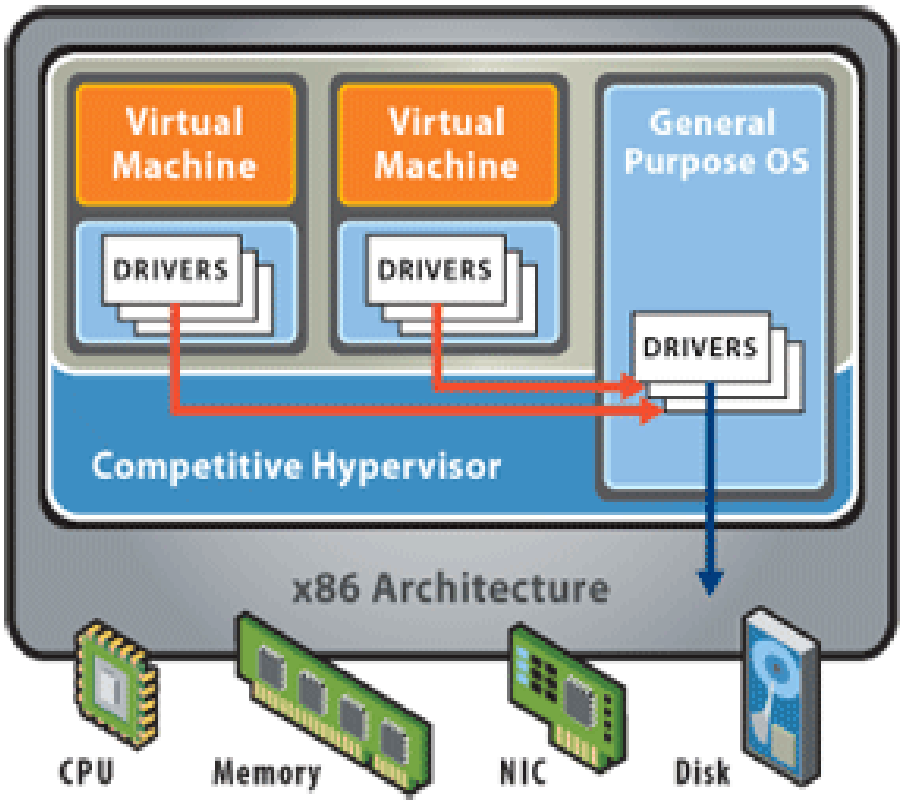


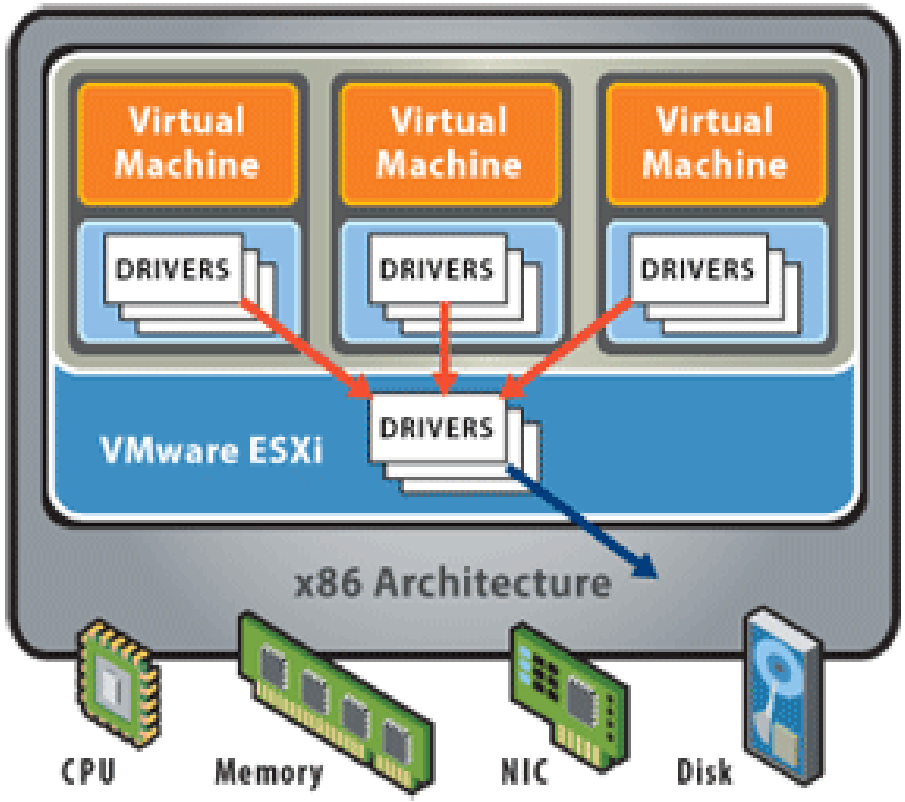
VM Architecture

- **Thin Virtualization – reduced size, independence**

=> Get Strong Security in a Small Package

  - the attack surface much smaller, and reduces the potential for vulnerabilities
  - far fewer interfaces to exploit and less malware threats





VM Architecture

- Security Concepts in Architecture
  - Extended computing stack
  - Guest isolation
  - Host Visibility from the Guest
  - Virtualized interfaces
  - Management interfaces
  - Greater co-location of data and assets on one box

VM Security Benefits

- Abstraction and Isolation
- Better Forensics and Faster Recovery After an Attack
- Patching is Safer and More Effective
- More Cost Effective Security Devices
- Future: Leveraging Virtualization to Provide Better Security

VM Security Issues

- VM Sprawl
- Mobility
- Hypervisor Intrusion
- Hypervisor Modification
- Communication
- Denial of Service

VM Security Issues

Issue	Hosted	Bare-Metal
Vulnerability of the underlying OS	susceptible to all the vulnerabilities and attacks that are prevalent on such systems.	a much smaller attack surface
Sharing of files and data between the guest and the host	vulnerable to data leakage and malicious code intrusion.	there is no mechanism share user information between virtual machines and their host.
Resource allocation	They are at the mercy of the host OS and other applications.	No single virtual machine can use all the resources or crash the system.
Target Usage	- is targeted for environments where the guest virtual machines can be trusted. (software development, testing, demonstration, and trouble-shooting.)	can potentially be exposed to malicious users and network traffic. Strong isolation and strict separation of management greatly reduce any risk of harmful activity going beyond the boundaries of the virtual machine.

VM Security Concerns

- Managing oversight and responsibility
- Patching and maintenance
- Visibility and compliance
- VM sprawl
- Managing Virtual Appliances

Summary

- Introduction To OS and OS Security
- System Security Planning
- The Components of an OS Security Environment
- Vulnerabilities of OS
- Secure an operating system
- Operating Systems Hardening
  - Linux/Unix Security
  - Windows Security
- Virtualization Security

Q & A