

CS 356 – Lecture 25 and 26

Operating System Security

Spring 2013

Review

- Chapter 1: Basic Concepts and Terminology
- Chapter 2: Basic Cryptographic Tools
- Chapter 3 – User Authentication
- Chapter 4 – Access Control Lists
- Chapter 5 – Database Security (skipped)
- Chapter 6 – Malicious Software
- Networking Basics (not in book)
- Chapter 7 – Denial of Service
- Chapter 8 – Intrusion Detection
- Chapter 9 – Firewalls and Intrusion Prevention
- Chapter 10 – Buffer Overflow
- Chapter 11 – Software Security
- Chapter 12 – OS Security



Chapter 12

Operating System Security

Operating System

- each layer of code needs measures in place to provide appropriate security services
- **each layer is vulnerable to attack from below if the lower layers are not secured appropriately**

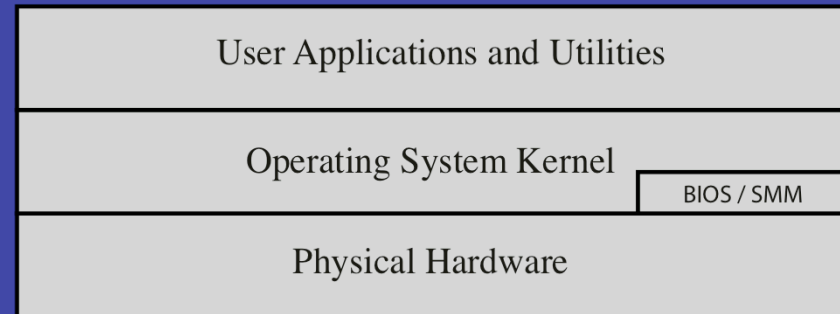


Figure 12.1 Operating System Security Layers

Security Layers

Measures

- the 2010 Australian Defense Signals Directorate (DSD) list the “Top 35 Mitigation Strategies”
- over 70% of the targeted cyber intrusions investigated by DSD in 2009 could have been prevented
- the top four measures for prevention are:
 - patch operating systems and applications using auto-update
 - patch third-party applications
 - restrict admin privileges to users who need them
 - white-list approved applications

Operating System Security

- possible for a system to be compromised during the installation process before it can install the latest patches
- building and deploying a system should be a planned process designed to counter this threat
- process must:
 - assess risks and plan the system deployment
 - secure the underlying operating system and then the key applications
 - ensure any critical content is secured
 - ensure appropriate network protection mechanisms are used
 - ensure appropriate processes are used to maintain security

System Security Planning

the first step in deploying a new system is planning

plan needs to identify appropriate personnel and training to install and manage the system

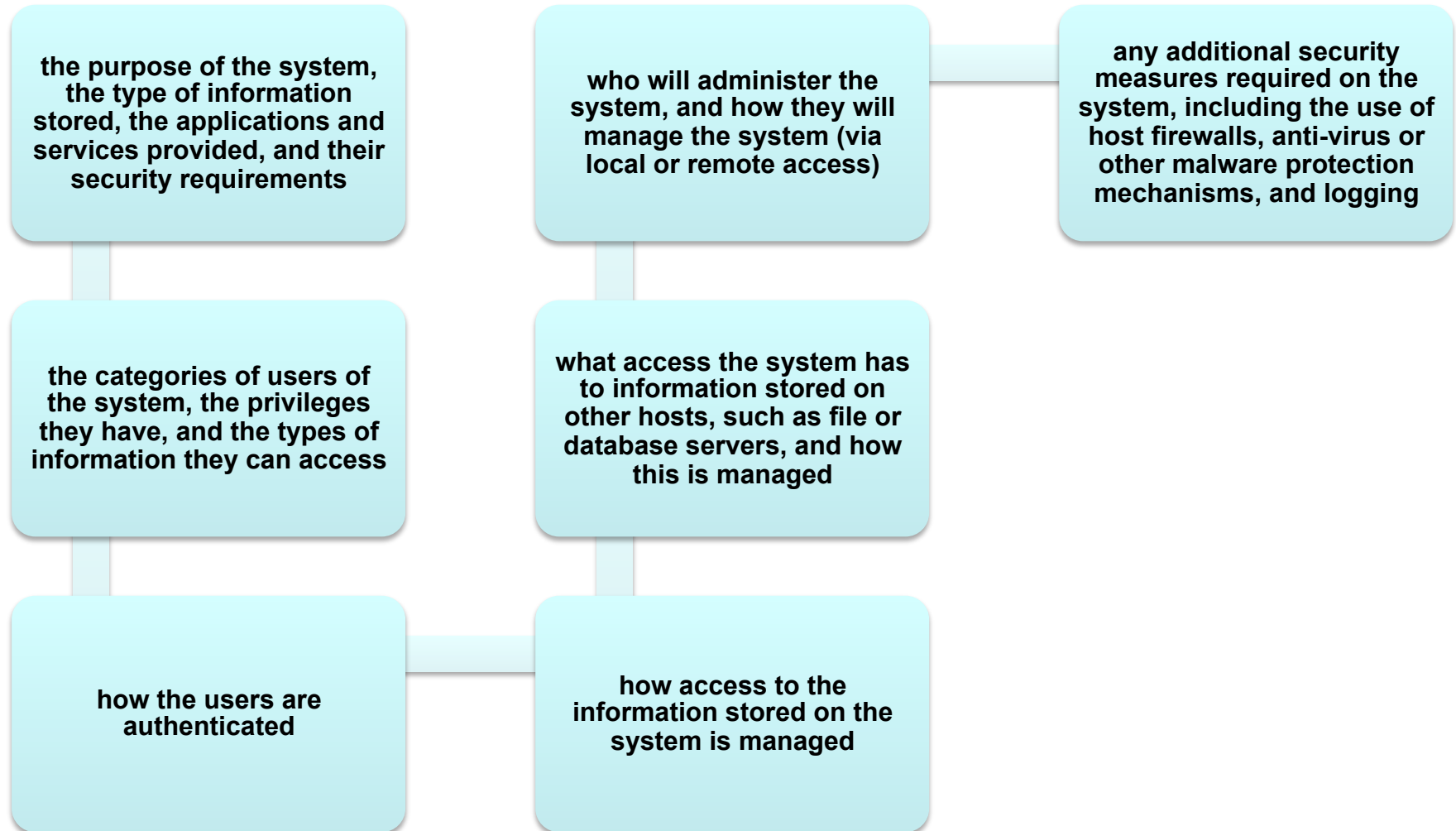
planning should include a wide security assessment of the organization

planning process needs to determine security requirements for the system, applications, data, and users

aim is to maximize security while minimizing costs



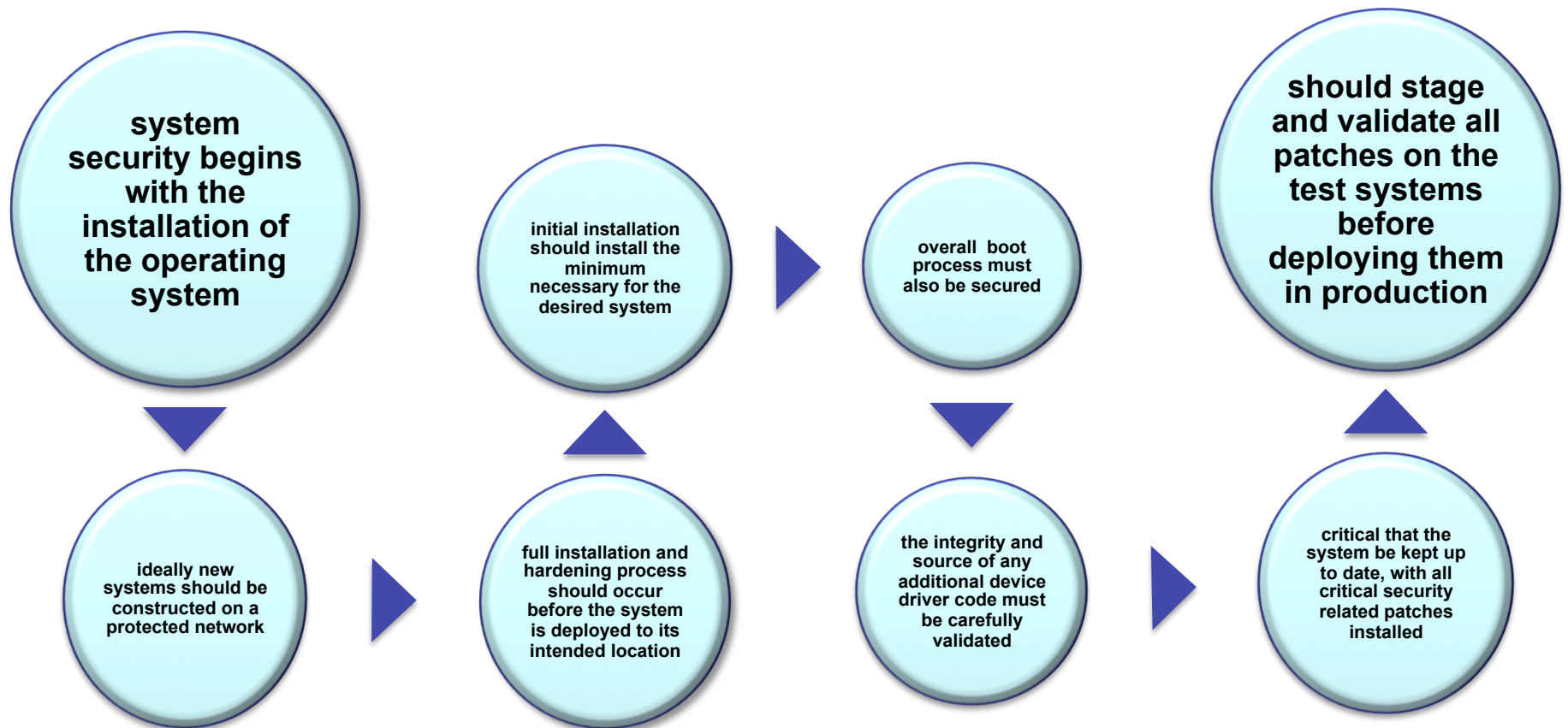
System Security Planning Process



Operating Systems Hardening

- first critical step in securing a system is to secure the base operating system
- basic steps
 - install and patch the operating system
 - harden and configure the operating system to adequately address the identified security needs of the system
 - install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)
 - test the security of the basic operating system to ensure that the steps taken adequately address its security needs

Initial Setup and Patching





- if fewer software packages are available to run the risk is reduced
 - system planning process should identify what is actually required for a given system
- when performing the initial installation the supplied defaults should not be used
 - default configuration is set to maximize ease of use and functionality rather than security
 - if additional packages are needed later they can be installed when they are required



- not all users with access to a system will have the same access to all data and resources on that system
- elevated privileges should be restricted to only those users that require them, and then only when they are needed to perform a task
- system planning process should consider:
 - categories of users on the system
 - privileges they have
 - types of information they can access
 - how and where they are defined and authenticated
- default accounts included as part of the system installation should be secured
 - those that are not required should be either removed or disabled
 - policies that apply to authentication credentials configured



- once the users and groups are defined, appropriate permissions can be set on data and resources
- many of the security hardening guides provide lists of recommended changes to the default access configuration



- further security possible by installing and configuring additional security tools:
 - anti-virus software
 - host-based firewalls
 - IDS or IPS software
 - application white-listing



- final step in the process of initially securing the base operating system is security testing
- goal:
 - ensure the previous security configuration steps are correctly implemented
 - identify any possible vulnerabilities
- checklists are included in security hardening guides
- there are programs specifically designed to:
 - review a system to ensure that a system meets the basic security requirements
 - scan for known vulnerabilities and poor configuration practices
- should be done following the initial hardening of the system
- repeated periodically as part of the security maintenance process

Application Configuration

- may include:
 - creating and specifying appropriate data storage areas for application
 - making appropriate changes to the application or service default configuration details
- some applications or services may include:
 - default data
 - scripts
 - user accounts
- of particular concern with remotely accessed services such as Web and file transfer services
 - risk from this form of attack is reduced by ensuring that most of the files can only be read, but not written, by the server

Encryption Technology

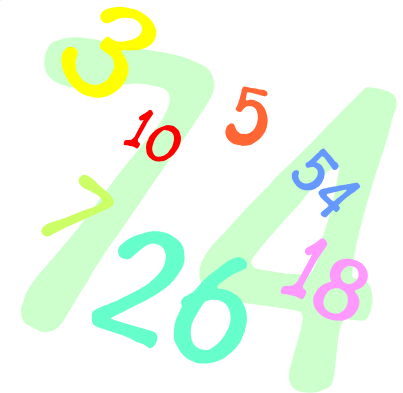
is a key enabling technology that may be used to secure data both in transit and when stored

must be configured and appropriate cryptographic keys created, signed, and secured

if secure network services are provided using TLS or IPsec suitable public and private keys must be generated for each of them

if secure network services are provided using SSH, appropriate server and client keys must be created

cryptographic file systems are another use of encryption



Security Maintenance

- process of maintaining security is continuous
- security maintenance includes:
 - monitoring and analyzing logging information
 - performing regular backups
 - recovering from security compromises
 - regularly testing system security
 - using appropriate software maintenance processes to patch and update all critical software, and to monitor and revise configuration as needed



Logging

automated analysis is preferred

can only inform you about bad things that have already happened

in the event of a system breach or failure, system administrators can more quickly identify what happened

key is to ensure you capture the correct data and then appropriately monitor and analyze this data

information can be generated by the system, network and applications

range of data acquired should be determined during the system planning stage

generates significant volumes of information and it is important that sufficient space is allocated for them

Data Backup and Archive

performing regular backups of data is a critical control that assists with maintaining the integrity of the system and user data

- may be legal or operational requirements for the retention of data

backup

- the process of making copies of data at regular intervals

archive

- the process of retaining copies of data over extended periods of time in order to meet legal and operational requirements to access past data

needs and policy relating to backup and archive should be determined during the system planning stage

- kept online or offline
- stored locally or transported to a remote site
- trade-offs include ease of implementation and cost versus greater security and robustness against different threats

Linux/Unix Security

- patch management
 - keeping security patches up to date is a widely recognized and critical control for maintaining security
- application and service configuration
 - most commonly implemented using separate text files for each application and service
 - generally located either in the /etc directory or in the installation tree for a specific application
 - individual user configurations that can override the system defaults are located in hidden “dot” files in each user’s home directory
 - most important changes needed to improve system security are to disable services and applications that are not required

Linux/Unix Security

- users, groups, and permissions
 - access is specified as granting read, write, and execute permissions to each of owner, group, and others for each resource
 - guides recommend changing the access permissions for critical directories and files
 - local exploit
 - software vulnerability that can be exploited by an attacker to gain elevated privileges
 - remote exploit
 - software vulnerability in a network server that could be triggered by a remote attacker

Linux/Unix Security

remote access controls

- several host firewall programs may be used
- most systems provide an administrative utility to select which services will be permitted to access the system

logging and log rotation

- should not assume that the default setting is necessarily appropriate



Linux/Unix Security

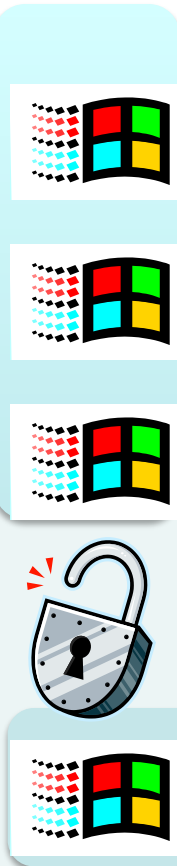
- chroot jail
 - restricts the server's view of the file system to just a specified portion
 - uses chroot system call to confine a process by mapping the root of the filesystem to some other directory
 - file directories outside the chroot jail aren't visible or reachable
 - main disadvantage is added complexity



Windows Security

patch management

- “Windows Update” and “Windows Server Update Service” assist with regular maintenance and should be used
- third party applications also provide automatic update support



users administration and access controls

- systems implement discretionary access controls resources
- Vista and later systems include mandatory integrity controls
- objects are labeled as being of low, medium, high, or system integrity level
- system ensures the subject's integrity is equal or higher than the object's level
- implements a form of the Biba Integrity model

Windows Security

Users Administration and Access Controls

Windows systems also define privileges

- system wide and granted to user accounts

combination of share and NTFS permissions may be used to provide additional security and granularity when accessing files on a shared resource

User Account Control (UAC)

- provided in Vista and later systems
- assists with ensuring users with administrative rights only use them when required, otherwise accesses the system as a normal user

Low Privilege Service Accounts

- used for long-lived service processes such as file, print, and DNS services

Windows Security

application and service configuration

- **much of the configuration information is centralized in the Registry**
 - **forms a database of keys and values that may be queried and interpreted by applications**
- **registry keys can be directly modified using the “Registry Editor”**
 - **more useful for making bulk changes**

Windows Security

- other security controls
 - essential that anti-virus, anti-spyware, personal firewall, and other malware and attack detection and handling software packages are installed and configured
 - current generation Windows systems include basic firewall and malware countermeasure capabilities
 - important to ensure the set of products in use are compatible
- Windows systems also support a range of cryptographic functions:
 - encrypting files and directories using the Encrypting File System (EFS)
 - full-disk encryption with AES using BitLocker
- “Microsoft Baseline Security Analyzer”
 - free, easy to use tool that checks for compliance with Microsoft’s security recommendations

Virtualization

- a technology that provides an abstraction of the resources used by some software which runs in a simulated environment called a virtual machine (VM)
- benefits include better efficiency in the use of the physical system resources
- provides support for multiple distinct operating systems and associated applications on one physical system
- raises additional security concerns

Virtualization Alternatives

application virtualization

allows applications written for one environment to execute on some other operating system

full virtualization

multiple full operating system instances execute in parallel

virtual machine monitor (VMM)

hypervisor

coordinates access between each of the guests and the actual physical hardware resources

Native Virtualization Security Layers

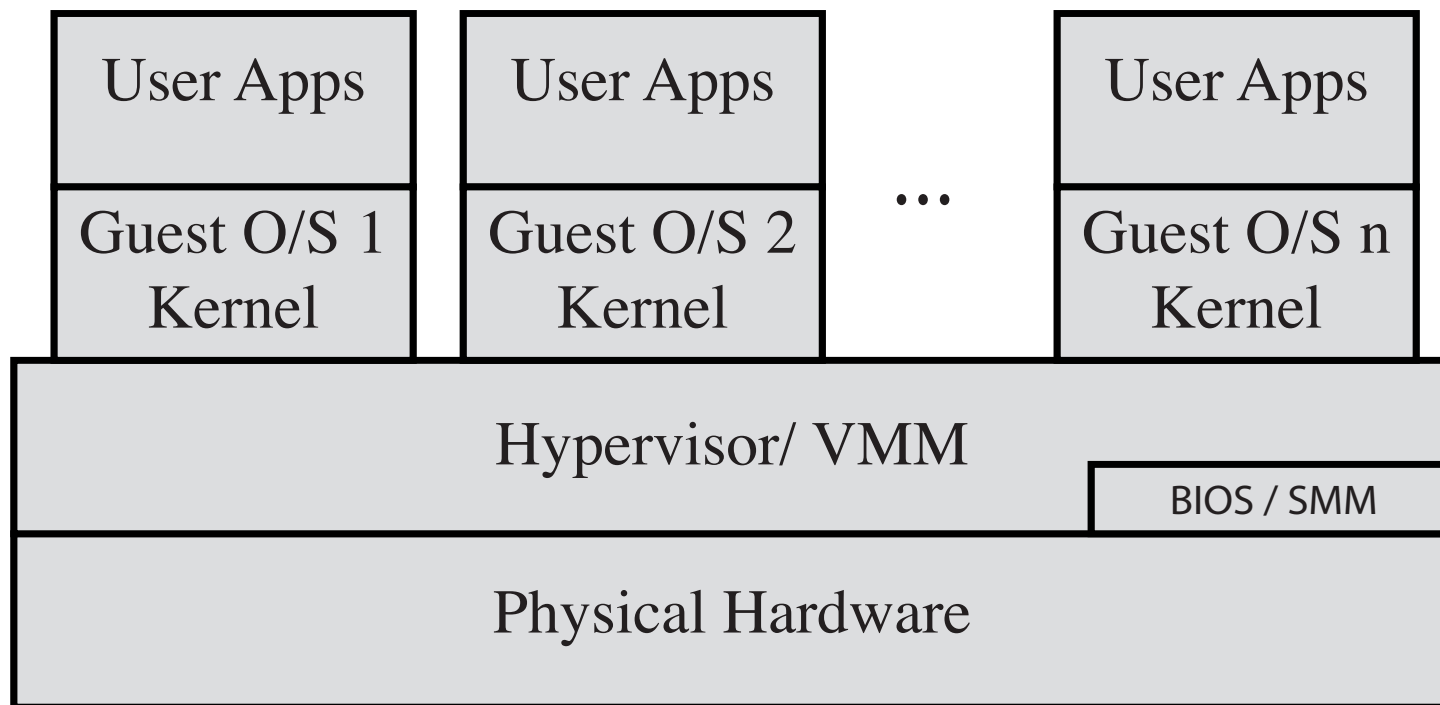


Figure 12.2 Native Virtualization Security Layers

Hosted Virtualization Security Layers

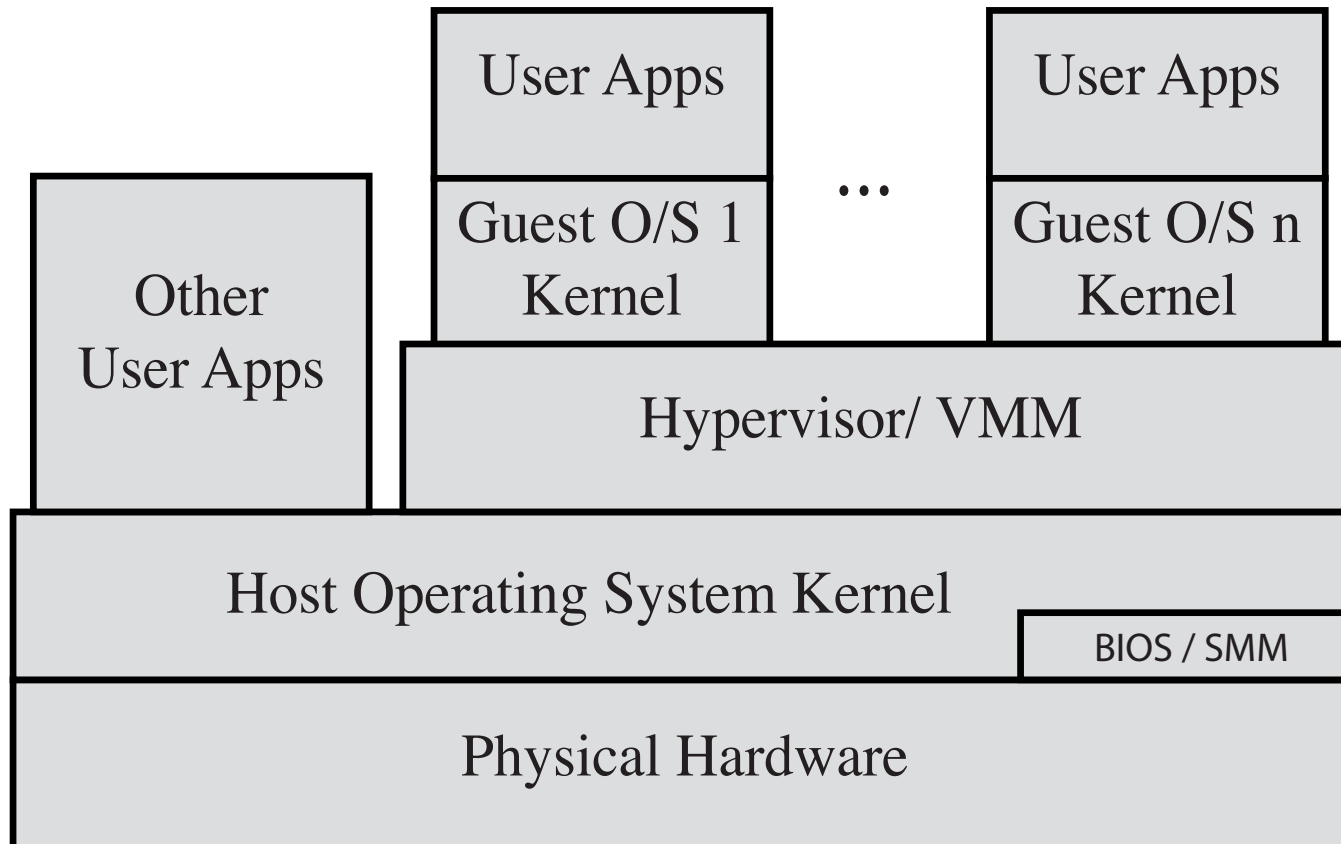



Figure 12.3 Hosted Virtualization Security Layers

Virtualization Security Issues

- security concerns include:
 - guest OS isolation
 - ensuring that programs executing within a guest OS may only access and use the resources allocated to it
 - guest OS monitoring by the hypervisor
 - which has privileged access to the programs and data in each guest OS
 - virtualized environment security
 - particularly image and snapshot management which attackers may attempt to view or modify

Securing Virtualization Systems



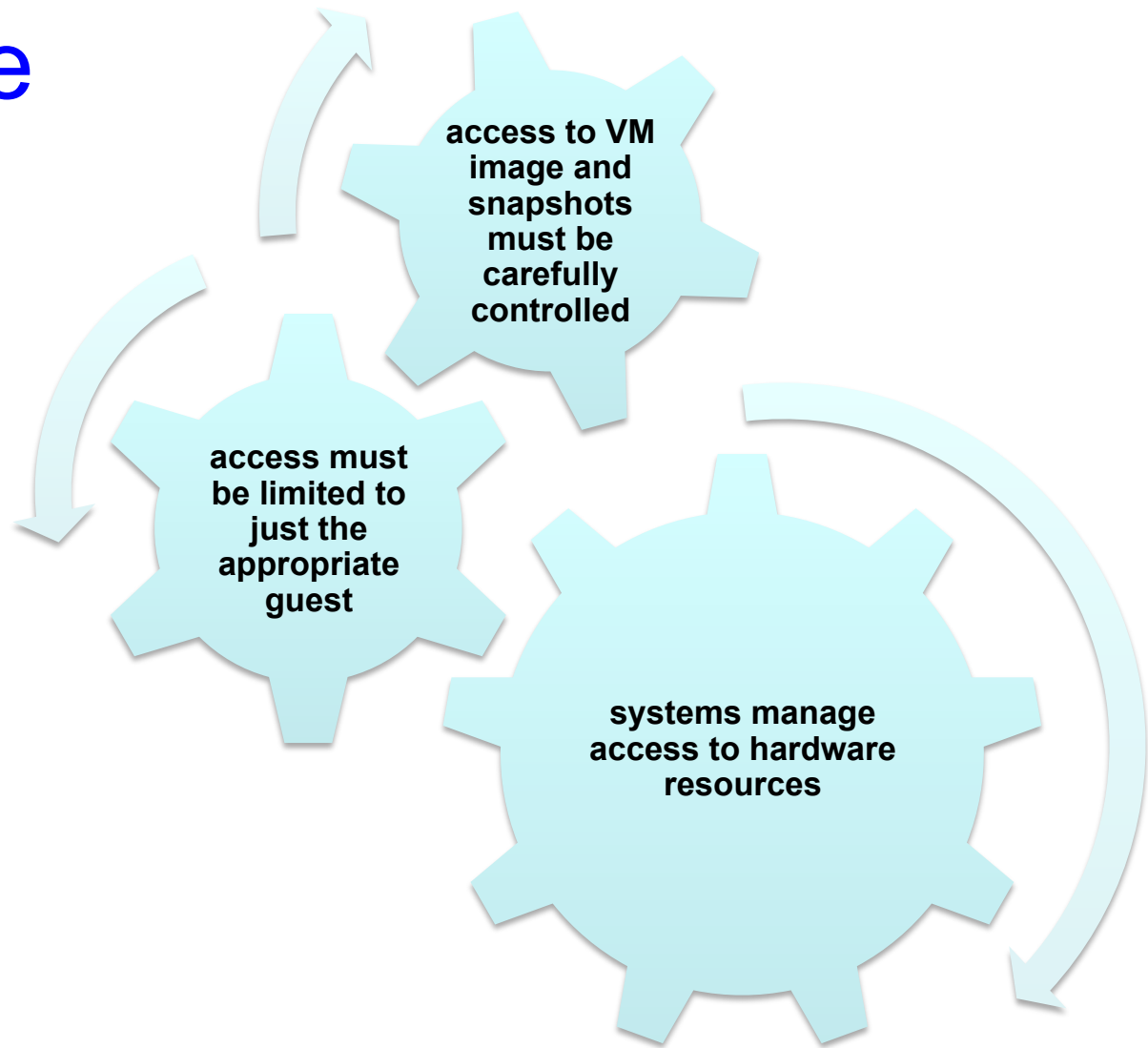
**organizations
using
virtualization
should:**

- **carefully plan the security of the virtualized system**
- **secure all elements of a full virtualization solution and maintain their security**
- **ensure that the hypervisor is properly secured**
- **restrict and protect administrator access to the virtualization solution**

Hypervisor Security

- should be
 - secured using a process similar to securing an operating system
 - installed in an isolated environment
 - configured so that it is updated automatically
 - monitored for any signs of compromise
 - accessed only by authorized administration
- may support both local and remote administration so must be configured appropriately
- remote administration access should be considered and secured in the design of any network firewall and IDS capability in use
- ideally administration traffic should use a separate network with very limited access provided from outside the organization

Virtualization Infrastructure Security





Summary

- system security planning
- operating systems hardening
 - initial setup and patching
 - remove unnecessary services
 - configure users and groups
 - test system security
- application security
 - application configuration
 - encryption technology
- security maintenance
 - data backup
- virtualization security
 - virtualization alternatives
- Linux/Unix security
 - patch management
 - application configuration
 - users, groups, permissions
 - remote access
 - security testing
- windows security
 - patch management
 - users administration and access controls
 - application and service configuration
 - security testing

