

IT 4823

Information Security Administration

Operating System Security



Notice: This session is
being recorded.

Some lecture slides prepared by Dr Lawrie Brown for “*Computer Security: Principles and Practice*”, 1/e, by William Stallings and Lawrie Brown.”.



Copyright © 2016 by Bob Brown

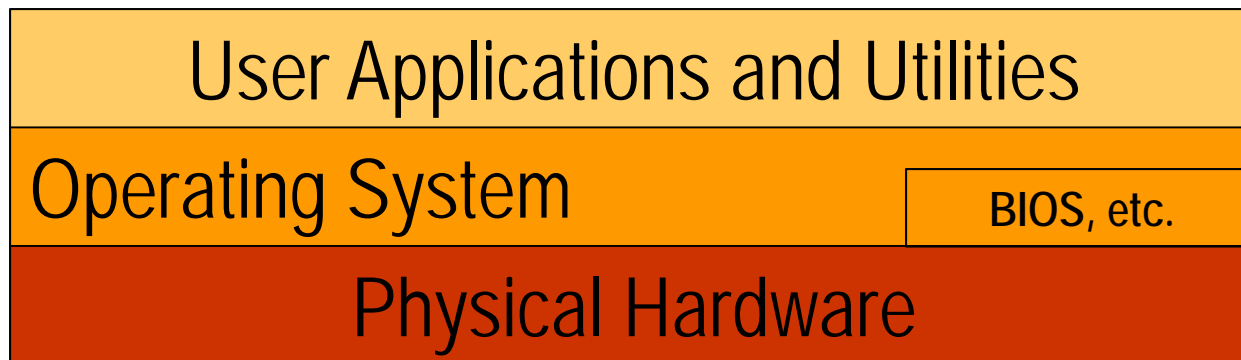


Next Week's Exam

- A few questions from exam one; no new material from the first third of the semester.
- Preparation:
 - Study exam one
 - Be sure you have read the assigned material
 - Review the slides
 - Look over the homework
 - Check podcasts for anything that's unclear.

Operating System

- Computer systems have at least three layers, of which the operating system is one.
- Each layer needs appropriate security measures.



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

Compromise During Installation

- It is 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

O.S. Security Planning

- The first step in deploying a new system is planning.
- The aim is to maximize security while minimizing costs.
- Planning process needs to determine security requirements for the system, applications, data, and users.
- 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 for Installation

- 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

NIST's Planning Information

1. The purpose of the system, the type of information stored, the applications and services provided, and their security requirements.
2. The categories of users of the system, the privileges they have, and the types of information they can access
3. How the users are authenticated
4. How access to the information stored on the system is managed.

NIST's Planning Information

5. What access the system has to information stored on other hosts, such as file or database servers, and how this is managed.
6. who will administer the system, and how they will manage the system (via local or remote access.)
7. What additional security measures are required on the system, including the use of host firewalls, anti-virus or other malware protection mechanisms, and logging

Operating Systems Hardening

- Secure the base operating system
- Basic steps:
 - Install and patch the operating system on a protected network.
 - Harden and configure the operating system to 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.
 - Test the security of the basic operating system to ensure that the steps taken adequately address its security needs.

Remove Unnecessary Services

- If fewer software packages are available to run, the risk is reduced.
- The system planning process should identify what is actually required for a given system (least privilege.)

Plan for Handling Supplied Defaults

- Default configurations are 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.
- Be especially careful about default passwords and access.

Plan for Authorization

- 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 (least privilege.)

Plan for Authentication/Authorization

- 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

Add, Configure Security Controls

- Once the users and groups are defined, set appropriate permissions 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

Test System Security

- 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

- Some applications or services may include:
 - default data
 - scripts
 - user accounts
- Of particular concern are 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

- Encryption is a key enabling technology that may be used to secure data both in transit and when stored
- Encryption must be configured and appropriate cryptographic keys created, signed, and secured
- If secure network services are provided using TLS, SSH, or IPsec suitable public and private keys must be generated for each of them
- 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

Plan for Logging

- A reactive control – can only tell about things that have already happened.
- Generates significant volumes of information, so it is important that sufficient space is allocated.
- The key is to ensure you capture the correct data and then appropriately monitor and analyze this data.
- Automated analysis is preferred.

Data Backup and Archive

- Two terms, three purposes:
- Backup
 - Immediate recovery of data accidentally or maliciously corrupted or deleted.
 - Disaster recovery in the event of damage to the data center.
- Archive: retaining copies of data over extended periods of time, months or years, in order to meet legal and operational requirements to access past data.

Data Backup

- Tension between requirements for immediate recovery and disaster recovery.
- Immediate recovery requires accessible backups.
- Disaster recovery requires off-site backups.
- It may be possible to transfer “delta” backups by network.
- Anything taken or sent off-site must be encrypted.

Data Archive

- Meets legal, regulatory, and operational requirements.
- It is important to be sure all required data are captured.
- Archived data that “age out” *must* be securely erased. (They can’t subpoena what you don’t have!)

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

About SETUID

- If the SETUID bit is on an executable file, when run it has the permissions of the file owner:

```
-r-sr-xr-x 1 root wheel 2531 May 1 sendmail
```

- Setting the SETGID bit gives the permissions of the group owner.
- Using SETUID / SETGID is *very dangerous!*
- A program with a vulnerability could be exploited at a higher level of privilege if SETUID / SETGID are set.

Linux/Unix Security

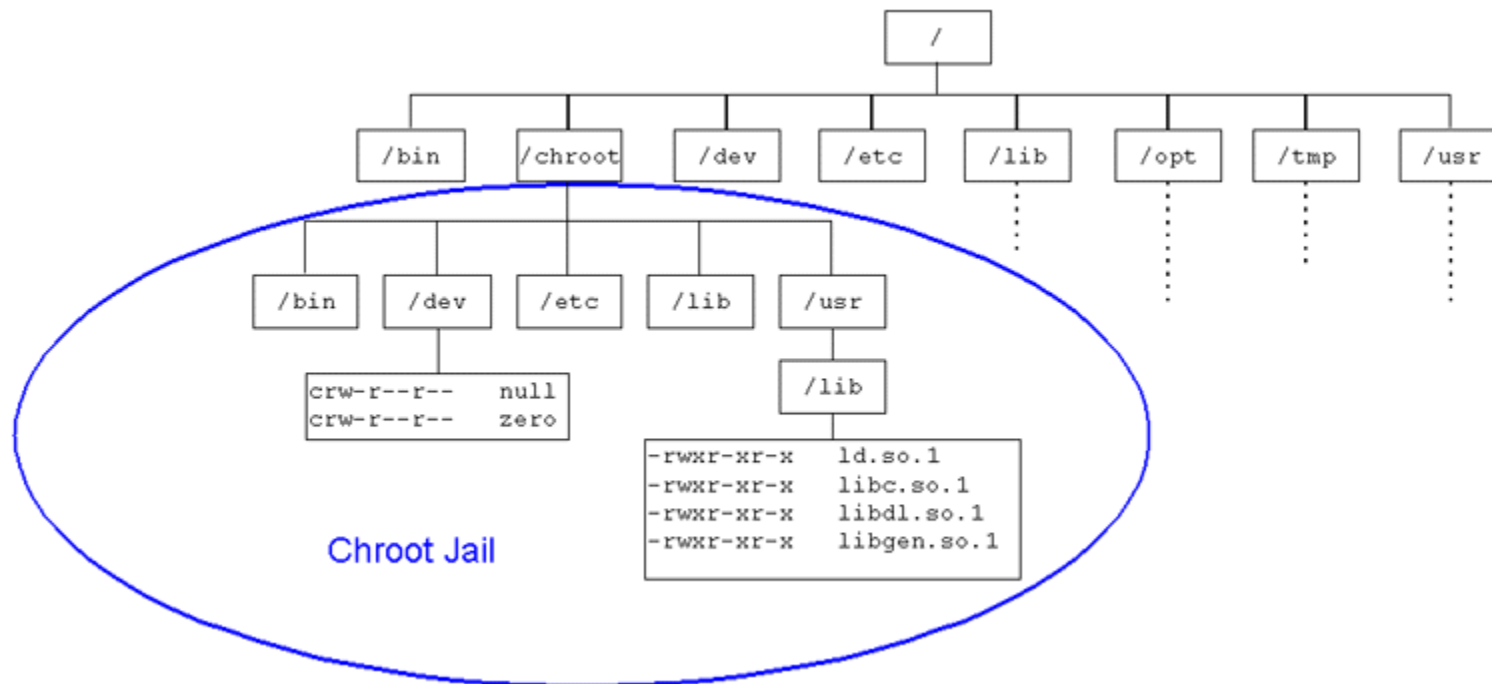
- Remote access controls:
 - several host firewall programs are available
 - most systems provide an administrative utility to select which services will be permitted to access the system
- logging and log rotation: do not assume that the default setting is necessarily appropriate.

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

Chroot Jail



Windows Patch Management

- “Windows Update” and “Windows Server Update Service” assist with regular maintenance and should be used when possible.
- It may be necessary to test patches before deployment.
- Most third party applications also provide automatic update support.

Windows User Administration and Access Control

- Windows implements discretionary access control for 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 User Administration and Access Controls

- Windows systems also define privileges system wide and granted to user accounts.
- 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
- Combination of share and NTFS permissions may be used to provide additional security and granularity when accessing files on a shared resource.

Windows Application and service Configuration

- Much of the configuration information is centralized in the Registry, a database of keys and values that may be queried and interpreted by applications
- Registry keys can be directly modified using the “Registry Editor”
- Many system services now run with lower privileges.

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
- “Microsoft Baseline Security Analyzer”
 - free, easy to use tool that checks for compliance with Microsoft’s security recommendations

Windows and Encryption

- 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
- Add-on encryption, such as VeraCrypt.

One Computer, More Than One OS?

- Running more than one operating system on a single hardware platform.
- We could run:
 - Applications that require different operating systems.
 - Applications that require special OS configurations.
- Reduced hardware requirements, and reduced complexity.
- We keep the CPUs busy.
- Doing so 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

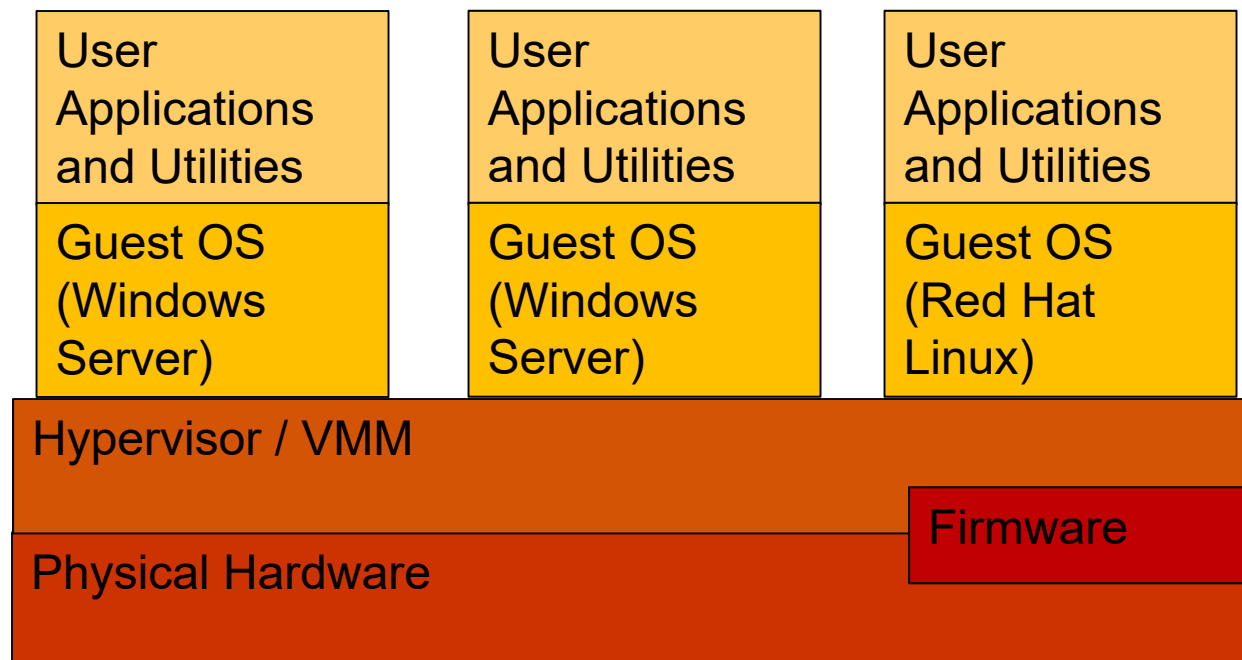
coordinates access between each of the guests and the actual physical hardware resources

Two Kinds of Virtual Machines

- Type I or Native
 - The hypervisor (virtual machine manager) runs directly on the hardware.
 - The hypervisor instantiates two or more virtual machines by abstracting the hardware interfaces.
 - Used mainly on servers
- Type II or Hosted
 - The virtual machine manager runs as an application of some other operating system
 - Used mostly on clients

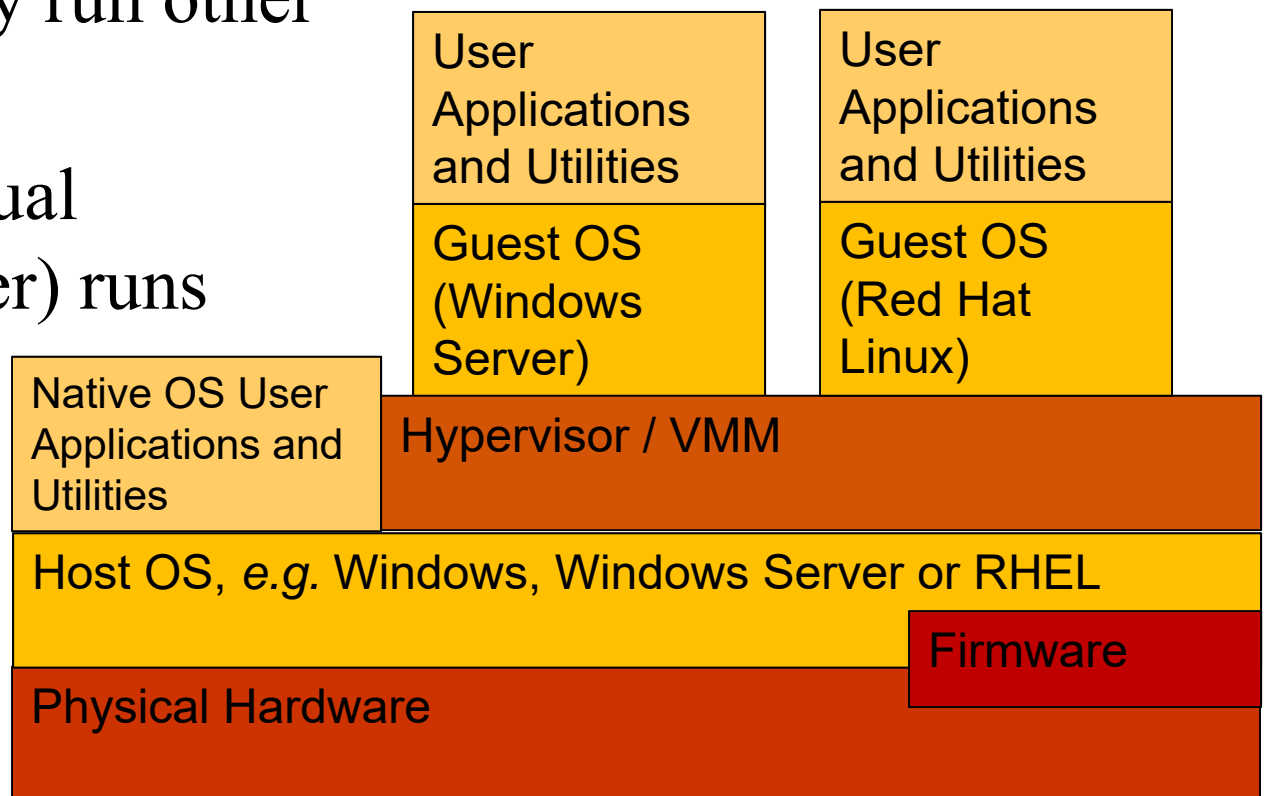
Type I (Native) Virtualization

- Hypervisor (Virtual Machine Manager) runs as the operating system for the hardware.
- Simulates (virtualizes) two or more computers, each of which can run its own operating system.



Type II (Hosted) Virtualization

- A standard operating system provides the hardware interface and may run other applications.
- Hypervisor (Virtual Machine Manager) runs as an application and virtualizes additional machines.



Planning: Virtualization Software

- There are many products available.
- The best product for an organization will depend on the nature of the organization.
- Choice of virtualization software will drive other planning decisions.
- Using multiple, different virtualization platforms multiplies complexity; a possible recipe for disaster.

Planning: Applications

- Are all applications supported in the selected virtual environment? Which ones are not?
- Application resources: Some resource-intensive applications and applications that require special hardware may not be good candidates for virtualization.
- Domain controllers, DNS servers, etc.: Particularly for Type II virtualization, Active Directory domain controllers, DNS servers, etc. may need to be running to start the host operating systems.

Planning: Hardware

- Physical hardware should have:
 - Fast, 64-bit CPUs
 - A *lot* of memory
 - Data center grade components.
- Virtualization may mean retiring and replacing older servers.

Planning: Capacity

- Capacity planning for data centers is more art than science.
- Running too many guest machines on a single physical machine will result in poor performance.
- Measure resources (CPU time, memory, disk, network throughput) on applications planned for virtualization.
- Don't forget that hypervisor and host OS (if used) will consume resources.
- Leave some slack.

Planning: Security

- Hypervisor / VMM security
 - Secure management functions, especially remote access.
 - Secure VM image and snapshot data.
 - Plan for applying hypervisor patches and upgrades.
- Guest and host OS security
 - Similar to security without virtualization.
 - Ensure that the hypervisor keeps guest OSs isolated.
 - Plan for OS patches and updates.

Virtualization Security Issues

- 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

Hypervisor Security

- The hypervisor 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

Questions

