Operating Systems Security

IT5306 Principles of Information Security

Level III - Semester 5

List of sub topics

1.1 System Security Planning

1.2 Operating Systems Hardening

1.3 Application Security

1.4 Security Maintenance

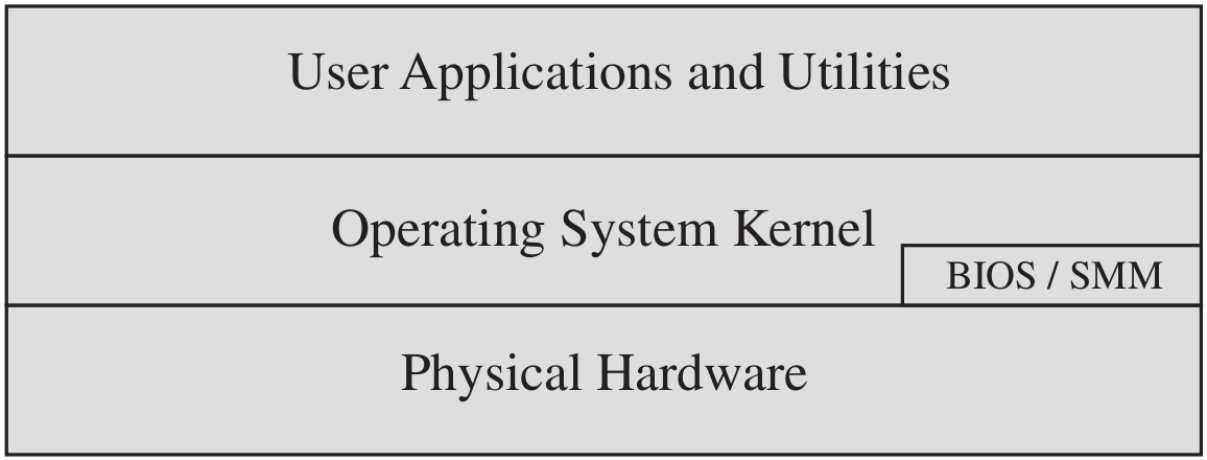
1.5 Linux/Unix Security

1.6 Windows Security

1.7 Virtualisation Security

1.1 System Security Planning

- A system can be viewed as a number of layers.
- Physical hardware at the bottom; the base operating system above including privileged kernel code, APIs, and services.
- User applications and utilities in the top layer.
- BIOS and possibly other code are external to the operating system kernel, but are used when booting the system or to support low-level hardware control.



1.1 System Security Planning

- Each layer needs security measures in place.

- Each layer is vulnerable to attack from below, should the lower layers not also be secured appropriately.

- Strategies to prevent targeted cyber intrusions.
  - White-list approved applications.
  - Patch third-party applications and operating system vulnerabilities.
  - Restrict administrative privileges.
  - Create a defense-in-depth system.

• Careful planning will help ensure that the new system is as secure as possible, and complies with any necessary policies.

1.1 System Security Planning

- The aim of the specific system installation planning process is to maximize security while minimizing costs.
- It is much more difficult and expensive to *retro-fit* security at a later time, than it is to plan and provide it during the initial deployment process.
- This planning process needs to determine the security requirements for the system, its applications and data, and of its users.
- This then guides the selection of appropriate software for the operating system and applications, and provides guidance on appropriate user configuration and access control settings.

1.1 System Security Planning

- Considerations during system security planning process :
  - The purpose of the system, the type of information stored, the applications and services provided, and their security requirements.
  - The categories of users of the system, the privileges they have, and the types of information they can access.
  - How the users are authenticated.
  - How access to the information stored on the system is managed.
  - What access the system has to information stored on other hosts, such as file or database servers, and how this is managed.
  - Who will administer the system, and how they will manage the system (via local or remote access).
  - Any additional security measures required on the system, including the use of host firewalls, anti-virus or other malware protection mechanisms, and logging.

1.2 Operating Systems Hardening

- A good security foundation needs a properly installed, patched, and configured operating system.
- Unfortunately, the default configuration for many operating systems often maximizes ease of use and functionality, rather than security.
- Further, since every organization has its own security needs, the appropriate security profile, and hence configuration, will also differ.
- While the details of how to secure each specific operating system differ, the broad approach is similar.

1.2 Operating Systems Hardening

- Basic steps to secure a raw operating system:
  - Install and patch the operating system.
  - Harden and configure the operating system to adequately address the identified security needs of the system to be deployed 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, host-based firewalls, and intrusion detection systems (IDS), if needed.
  - Test the security of the basic operating system to ensure that the steps taken adequately address its security needs.

1.3 Application Security

- Once the base operating system is installed and appropriately secured, the required services and applications must next be installed and configured.
- Install software on the system that is required to meet its desired functionality, in order to reduce the number of places vulnerabilities may be found.
- Software that provides remote access or service is of particular concern, since an attacker may be able to exploit this to gain remote access to the system.
- Each selected service or application must be installed, and then patched to the most recent supported secure version appropriate for the system. As with the base operating system, utilizing an isolated, secure build network is preferred.

1.3 Application Security

- Once installed, any application-specific configuration is performed.
- Some applications or services may include default data, scripts, or user accounts. These should be reviewed, and only retained if required, and suitably secured.
- As part of the configuration process, careful consideration should be given to the access rights granted to the application.
- Encryption is a key enabling technology that may be used to secure data both in transit and when stored.
- If secure network services are provided, most likely using either TLS or IPsec, then suitable public and private keys must be generated for each of them.

1.4 Security Maintenance

- Once the system is appropriately built, secured, and deployed, the process of maintaining security is continuous.
- This results from the constantly changing environment, the discovery of new vulnerabilities, and hence exposure to new threats.
- The process of 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

1.4 Security Maintenance - logging information

- Logging is a reactive control that can only inform you about bad things that have already happened.
- But effective logging helps ensure that in the event of a system breach or failure, system administrators can more quickly and accurately identify what happened and thus most effectively focus their remediation and recovery efforts.
- Logging information can be generated by the system, network, and applications. The range of logging data acquired should be determined during the system planning stage, as it depends on the security requirements and information sensitivity of the server.
- Manual analysis of logs is tedious and is not a reliable means of detecting adverse events. Rather, some form of automated analysis is preferred, as it is more likely to identify abnormal activity.

1.4 Security Maintenance - backups

- Performing regular backups of data on a system is another critical control that assists with maintaining the integrity of the system and user data.
- **Backup** is the process of making copies of data at regular intervals, allowing the recovery of lost or corrupted data over relatively short time periods of a few hours to some weeks.
- **Archive** is the process of retaining copies of data over extended periods of time, being months or years, in order to meet legal and operational requirements to access past data.
- The needs and policy relating to backup and archive should be determined during the system planning stage. Key decisions include whether the backup copies are kept online or offline, and whether copies are stored locally or transported to a remote site.

1.5 Linux/Unix Security

- Modern Unix and Linux distributions typically include tools for automatically downloading and installing software updates.
- It is important to configure whichever update tool is provided on the distribution in use, to install at least critical security patches in a timely manner.
- Configuration of applications and services on Unix and Linux systems is most commonly implemented using separate text files for each application and service.
- The name, format, and usage of these files are very much dependent on the particular system version and applications in use.
- Hence the systems administrators responsible for the secure configuration of such a system must be suitably trained and familiar with them.

1.5 Linux/Unix Security

- Unix and Linux systems implement discretionary access control to all file system resources.
- These include not only files and directories but devices, processes, memory, and indeed most system resources.
- Access is specified as granting read, write, and execute permissions to each of owner, group, and others, for each resource. These are set using the chmod command.
- In order to partition access to information and resources on the system, users need to be assigned to appropriate groups granting them any required access.
- It is widely accepted that the number and size of setuid root programs in particular should be minimized. They cannot be eliminated, as superuser privileges are required to access some resources on the system.

1.5 Linux/Unix Security

- Some network accessible services do not require access to the full file-system, but rather only need a limited set of data files and directories for their operation.
- Unix and Linux systems provide a mechanism to run such services in a chroot jail??, which restricts the server's view of the file system to just a specified portion.
- Chrooting therefore helps contain the effects of a given server being compromised or hijacked.

1.6 Windows Security

- Microsoft Windows systems have for many years formed a significant portion of all general purpose system installations.
- Hence, they have been specifically targeted by attackers, and consequently security countermeasures are needed to deal with these challenges.
- The “Windows Update” service and the “Windows Server Update Services” assist with the regular maintenance of Microsoft software, and should be configured and used.
- Many other third-party applications also provide automatic update support, and these should be enabled for selected applications.

1.6 Windows Security

- Users and groups in Windows systems are defined with a Security ID (SID).
- It may also be centrally managed for a group of systems belonging to a domain, with the information supplied by a central Active Directory (AD) system using the LDAP protocol.
- Windows systems implement discretionary access controls to system resources such as files, shared memory, and named pipes.
- The access control list has a number of entries that may grant or deny access rights to a specific SID, which may be for an individual user or for some group of users.

1.6 Windows Security

- Windows Vista and later systems also include mandatory integrity controls.
- These label all objects, such as processes and files, and all users, as being of low, medium, high, or system integrity level.
- Then whenever data is written to an object, the system first ensures that the subject's integrity is equal or higher than the object's level.
- Windows systems also define privileges, which are system wide and granted to user accounts.
- Examples of privileges include the ability to backup the computer (which requires overriding the normal access controls to obtain a complete backup), or the ability to change the system time.

1.6 Windows Security

- Unlike Unix and Linux systems, much of the configuration information in Windows systems is centralized in the Registry, which forms a database of keys and values that may be queried and interpreted by applications on these systems.
- Changes to these values can be made within specific applications, setting preferences in the application that are then saved in the registry using the appropriate keys and values.
- It is essential that suitable anti-virus, anti-spyware, personal firewall, and other malware and attack detection and handling software packages are installed and configured on such systems.
- Windows systems also support a range of cryptographic functions that may be used where desirable, e.g., Encrypting File System (EFS), and for full-disk encryption with AES using BitLocker.

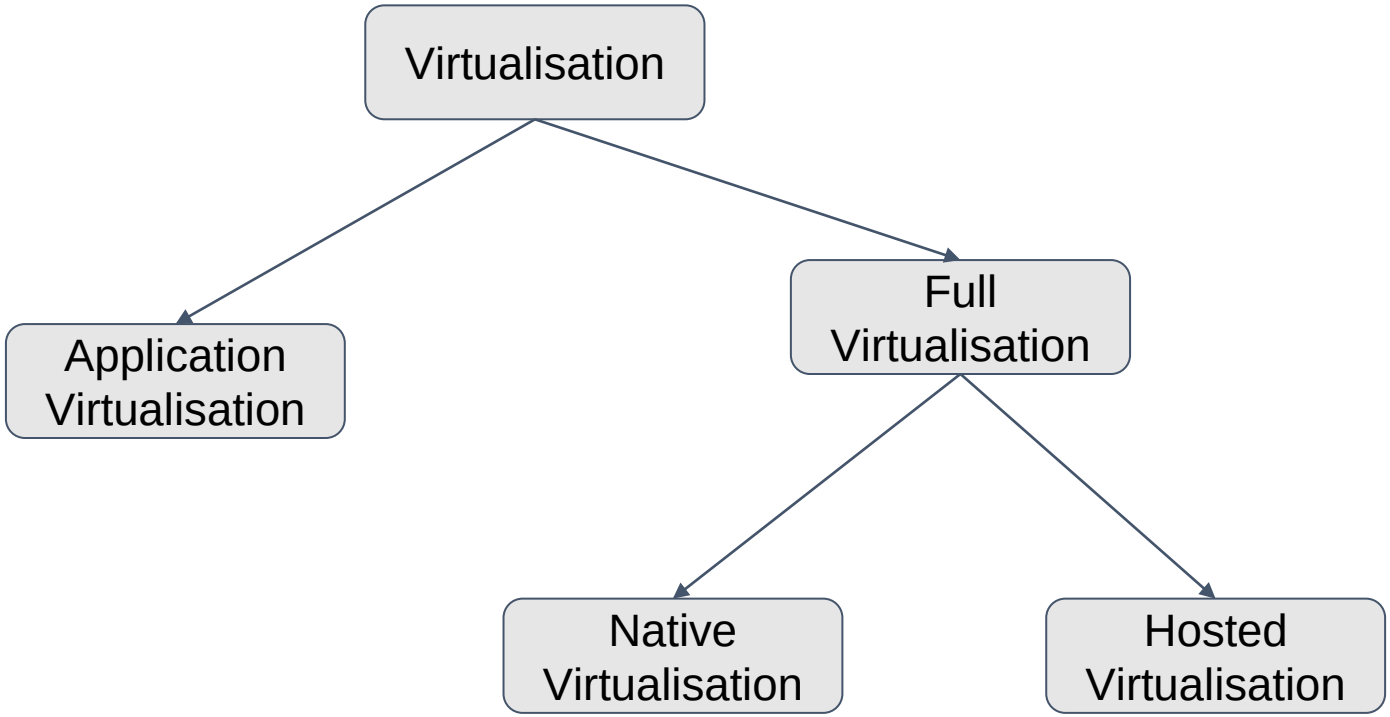
1.7 Virtualisation Security

- Virtualization refers to a technology that provides an abstraction of the computing resources used by some software, which thus runs in a simulated environment called a virtual machine (VM).

- This allows multiple full operating system instances to execute on virtual hardware, supported by a hypervisor that manages access to the actual physical hardware resources.

- There are a number of additional security concerns raised in virtualized systems, as a consequence both of the multiple operating systems executing side by side and of the presence of the virtualized environment and hypervisor as a layer below the operating system kernels and the security services they provide.

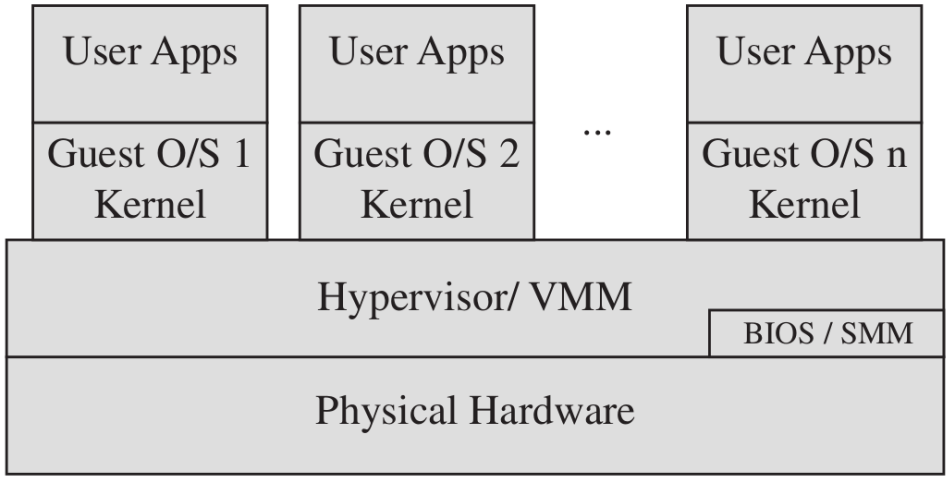
1.7 Virtualisation Security



Application virtualisation: Allows applications written for one environment, to execute on some other operating system.

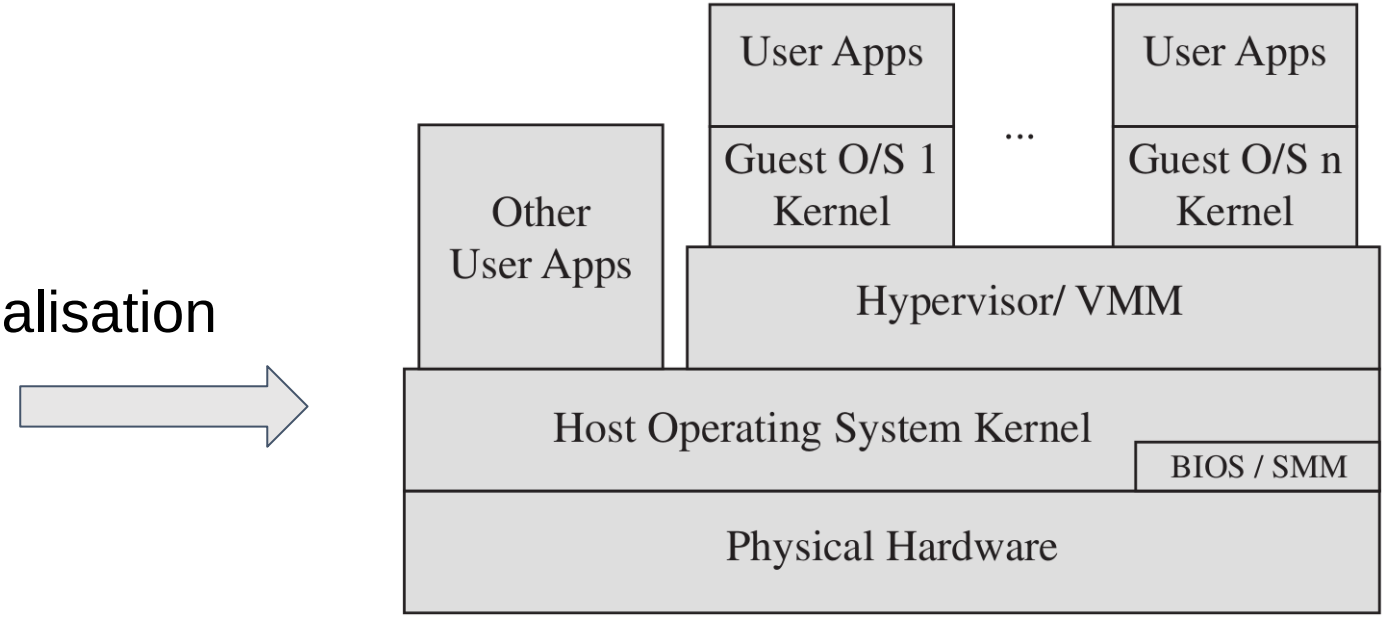
Full virtualisation: Multiple full operating system instances execute in parallel.

1.7 Virtualisation Security



Native virtualisation

Hosted virtualisation



1.7 Virtualisation Security

- Virtualization security issues:
  - Guest OS isolation, ensuring that programs executing within a guest OS may only access and use the resources allocated to it, and not covertly interact with programs or data either in other guest OSs or in the hypervisor.
  - Guest OS monitoring by the hypervisor, which has privileged access to the programs and data in each guest OS, and must be trusted as secure from subversion and compromised use of this access.
  - Virtualized environment security, particularly image and snapshot management, which attackers may attempt to view or modify.

1.7 Virtualisation Security

- Organizations using virtualization should:
  - Carefully plan the security of the virtualized system.
  - Secure all elements of a full virtualization solution, including the hypervisor, guest OSs, and virtualized infrastructure, and maintain their security.
  - Ensure that the hypervisor is properly secured.
  - Restrict and protect administrator access to the virtualization solution.