Course: Information Security Management in e-Governance

Day 1

Session 5: Securing Data and Operating systems

Agenda

- Introduction to information, data and database systems
- Information security risks surrounding data and database systems
- Information security considerations and solutions for data and database systems

Terms & Concepts : What is a Database?

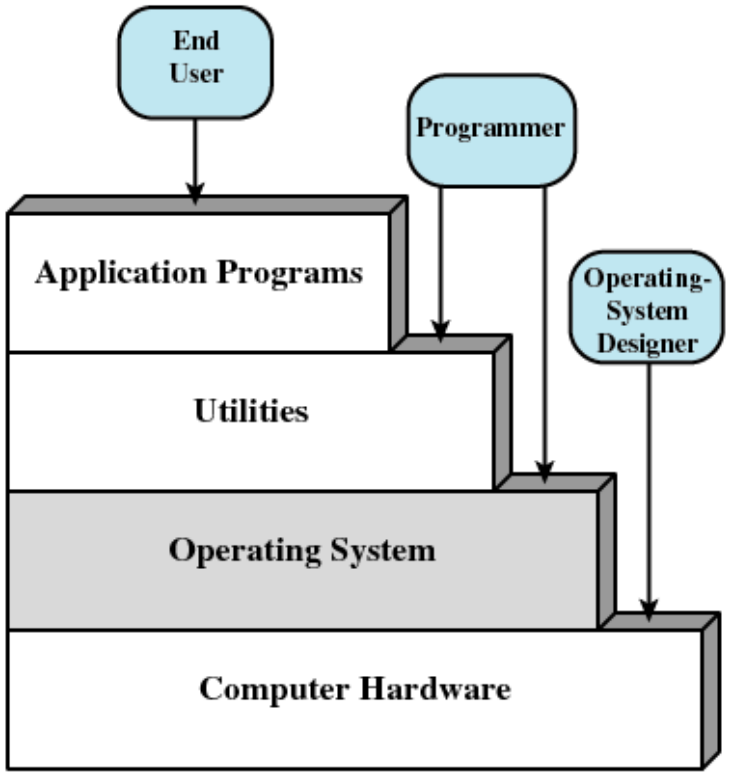
- An organized collection of information
  - A database can also be defined as a collection of information represented in coded data elements and specific relationships between those data elements
  - Databases are cardinal components of any application which enables provision of dynamic content and is shared across users, uses and applications
- Usually in the form of
  - Fields: a single value / piece of information; like a 'cell' in Excel
  - Records: a complete set of information; composed of fields (a "row")
  - File (or table): a set of records
- DBMS (Database Management System)
  - basically the software that manages your database

Operating Systems

What is an operating system?

The operating system can be considered in various ways:

- an intermediary between the user software and the hardware
- an abstraction layer providing an idealized view of the computer hardware
- a virtual machine
- a set of services



The leading risks and threats

Risks to your computer's security include:

- Viruses
- Worms
- Trojans
- Spyware

Operating system security

- OS is responsible for ensuring that the users are securely authenticated and controlled
- Operating system comes with many security vulnerabilities
- Firewall stops most Internet based attacks, however, they cannot stop all outside attacks
- Firewalls are less effective for attacks within the corporation
- Operating system security is required to achieve the three basic objectives of security (CIA): Confidentiality, Integrity and Availability.

Keep Your Operating System Updated

- Just keep your system up to date with the latest software available.
- Online criminals are constantly at work devising new ways to attack your computer and invade your privacy. Fortunately, software companies work even harder to counter those threats and to provide you with updated tools that you can use to protect your PC.
- You should regularly update your computer operating system with security updates provided by the manufacturer. The same goes for your Web browser and other important applications, including your antivirus and antispyware programs

The Benefits of Automatic Security Updates

- As with human viruses, the best treatment for computer viruses is to avoid getting them in the first place.
- Having up-to-date security features already installed as part of your computer system helps to ensure that you have the highest level of protection available.
- And because security software is continually updated to anticipate and respond to new and evolving threats, the easiest way to ensure that you have the latest security enhancements is to schedule automatic updates for your computer.

Install and Maintain Antivirus Software

- Antivirus software helps to protect your computer by scanning every e-mail, application or piece of content that enters your PC.
- Strong antivirus programs can detect and destroy thousands of specific viruses before they have a chance to damage your system.
- Online attackers are constantly creating new viruses and worms, and devising new ways to invade and damage your computer.
- To protect your PC from these threats, make sure you never let your antivirus program expire, and keep the software up to date with the latest updates from the manufacturer.

Install and Maintain Antispyware Software

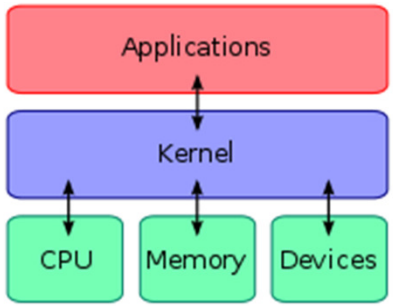
- Antispyware software can expose any spies already on your system, and help to keep your computer running smoothly and prevent further intrusion.
- As with your operating system and antivirus software, it is essential that you keep your antispyware software updated to make sure you have the highest level of protection for your PC.

Need for Operating systems hardening

- Host hardening makes it difficult to attack on a host systems.

- A hardened OS is one in which the vendor has modified the kernel source code to provide for a mechanism, which provides a security perimeter between the non – secure application software, the secure application software and network stack

- A kernel connects the application software to the hardware of a computer



OS hardening fundamentals

Following are the fundamental steps for OS hardening

Do a disconnected install

- During installation of an OS , disconnect from any network, especially the internet
- Best practice suggest to download the necessary patches and then apply these downloaded patches to the machines

Lock down the OS

- Install all applicable patches and updates (in the form of service packs or updated releases)
- Update the OS on regular basis

OS hardening fundamentals

Lock down the services:

- All services and third party programs on the computer should be checked to ensure that they are the most current versions
- Lock down the services which are not required on the machine

Define a proper baseline

- Once the IT system is patched and locked down next step is to establish a baseline for IT systems
- This is mostly to ensure that a proper documentation of changes that were carried out on the IT system exists
- If any changes are made to the baselines , it can be verified and appropriate security measures can be taken

Some other measures for Operating System Security

Some of the measures are listed below

- Provide physical security to the host
- Install the OS with secure configuration options
- Download and install patches for know vulnerabilities
- Turn off unnecessary services and hardening all remaining applications
- Manage users and groups
- Manage access permission
- Regular server backup

Some of the measures for Host Hardening

- Patch and update the OS
- Identify vulnerabilities
- Mitigate if necessary
- Patch servers in isolation
- Test patches before applying (depends upon availability of test environment)
- Harden and configure the OS
- Disable and remove unnecessary services or applications
- Configure user authentication
- Configure resource controls
- Install and configure additional security controls
- Anti-malware –End-point Security
- Host based firewalls to block unwanted open ports
- Host based intrusion detection (HIDS) system
- Patch management software
- Test the security of OS

Additional operating system access controls

Additional operating system access controls include the following actions:

- Ensure system administrators and security professionals have adequate expertise to securely configure and manage the operating system.
- Ensure effective authentication methods are used to restrict system access to both users and applications.
- Activate and utilize operating system security and logging capabilities and supplement with additional security software where supported by the risk assessment process.
- Restrict operating system access to specific terminals in physically secure and monitored locations.

Additional operating system access controls (cont'd)

- Lock or remove external drives from system consoles or terminals residing outside physically secure locations.
- Restrict and log access to system utilities, especially those with data altering capabilities.
- Restrict access to operating system parameters.
- Prohibit remote access to sensitive operating system functions, where feasible, and at a minimum require strong authentication and encrypted sessions before allowing remote support.

Additional operating system access controls (cont'd)

- Limit the number of employees with access to sensitive operating systems and grant only the minimum level of access required to perform routine responsibilities.
- Segregate operating system access, where possible, to limit full or root level access to the system.
- Monitor operating system access by user, terminal, date, and time of access.
- Update operating systems with security patches and using appropriate change control mechanisms.

End of Session