Chapter 17 Questions

Questions may be asked in class, on quizzes, and on exams

Students will be able to:

* + **define the concept of protection as pertains to a computer**
* Computer security, also known as network security or IT security, is protecting information systems from theft or damage to hardware, software, and information, as well as from interrupting or misleading the services they provide.
  + explain the difference between a policy and a mechanism and provide an example
* A policy is a method of choosing which activities to perform.
* A mechanism is an implementation of an enforcement policy, usually to some extent dependent on the hardware on which the operating system runs.
* For example, a first-come-first-served policy can be used to grant resources to a process
  + explain the principle of least privilege, and provide an example that is not related to computers
* The principle of least privilege is one of the most basic principles in system security.
* Least Privilege refers to "the Privilege that is essential for every subject (user or process) on the network to perform an operation".
* The principle of minimum privilege refers to "the minimum privilege necessary for each subject in the network to ensure the minimum loss caused by possible accidents, errors, tampering of network components, etc.".
  + **for purposes of using an Access Matrix, explain what the Domain component is or represents, and explain what the Object component is or represents**
* The domain component (DC) refers to each component of the domain.
* For example, www.gerardnico.com can be written as DC= WWW,DC=gerardnico,DC=com
  + with respect to Access Matrices, explain the difference between an Access List for Objects and a Capability List for Domains
* An access list is a list of each object, consisting of fields that have a non-empty access set for that object.
* The access list for the object lists the fields that contain access to the object.
* For each domain, the function list describes the access rights of each object in that domain.
* The difference between the two structures is in how their information is organized.
* Access lists are organized by objects (columns in the access matrix), and function lists are organized by fields (rows in the access matrix).
  + explain Role Based Access Control and provide an example
* Role-based Access Control (RBAC) is a method of restricting network access based on the role of a single user in an enterprise.
* RBAC allows employees to access only what they need to do their job and prevents them from accessing information that is not relevant to them
* Example : Low-level users only have the right to write files to high-level users, but they do not have the right to obtain files from high-level users (as is the case in general military systems). This ensures the flow of information, that is, from low-level to high-level, thus ensuring the security of information.
  + **explain why a system might need to relinquish or revoke access rights, and provide an example**
* When the system is attacked, in order to protect the internal data information of the system, the access permission should be revoked or destroyed to protect the data
* When a communications company is attacked, they revoke or destroy access rights to protect customer information
  + **explain the potential difficulties with removing access to a resource**
* There may still be some data information left behind, that is, not completely deleted or undone clean
  + explain the meaning of using a sandbox in computers, and provide an example
* In computer security, a sandbox is a security mechanism that separates running programs, usually to reduce the spread of system failures and/or software vulnerabilities.
* Network access, the ability to check host systems or read from input devices is usually prohibited or severely restricted.
* Example The sandbox can redirect the software operation files, registry and other paths in the sandbox to other locations (the location specified by the sandbox), so that the resources intended to be operated by the software will not be accessed or operated, ensuring the security of the resources.
  + explain how language-based protection is implemented, and **provide an example using the Java programming language**
* Language-based security (LBS) is a set of technologies that can be used to enhance application security at a higher level by using programming language attributes. LBS is considered to enforce computer security at the application level, thus potentially preventing vulnerabilities that traditional operating system security cannot handle
* For example : Database access based on Java language, Implement SMS encryption based on Java language, Network encryption based on JAVA language
  + End of Chapter 17
    - no end of chapter questions