Module-1

Types of Controls in Information Security

Controls in Information Security

- Once an organization defines control objectives, it can assess the risk to individual assets and then choose the most appropriate security controls to put in place.

Control Types

- Physical controls
- Technical controls
- Administrative controls

Control Types

- Physical controls

Control Types

- Physical controls
  - It describe anything tangible that's used to prevent or detect unauthorized access to physical areas, systems, or assets. This includes things like fences, gates, guards, security badges and access cards, biometric access controls, security lighting, CCTVs, surveillance cameras, motion sensors, fire suppression, as well as environmental controls like HVAC and humidity controls.

Control Types

- Technical controls

Control Types

- Technical controls
  - (also known as logical controls) include hardware or software mechanisms used to protect assets. Some common examples are authentication solutions, firewalls, antivirus software, intrusion detection systems (IDSs), intrusion protection systems (IPSs), constrained interfaces, as well as access control lists (ACLs) and encryption measures.

Control Types

- Administrative controls

Control Types

- Administrative controls
  - It refer to policies, procedures, or guidelines that define personnel or business practices in accordance with the organization's security goals. These can apply to employee hiring and termination, equipment and Internet usage, physical access to facilities, separation of duties, data classification, and auditing. Security awareness training for employees also falls under the umbrella of administrative controls.

Security Control Functions

- Preventative controls
- Detective controls
- Corrective controls
- Recovery controls
- Compensation controls

Security Control Functions

- Preventative controls
  - It describe any security measure that's designed to stop unwanted or unauthorized activity from occurring.
  - Examples include physical controls such as fences, locks, and alarm systems;
  - technical controls such as antivirus software, firewalls, and IPSs; and
  - administrative controls like separation of duties, data classification, and auditing.

Security Control Functions

- Detective controls
  - It describe any security measure taken or solution that's implemented to detect and alert to unwanted or unauthorized activity in progress or after it has occurred.
  - Physical examples include alarms or notifications from physical sensor (door alarms, fire alarms) that alert guards, police, or system administrators.
  - Honeypots and IDSs are examples of technical detective controls.

Security Control Functions

- Corrective controls
  - It include any measures taken to repair damage or restore resources and capabilities to their prior state following an unauthorized or unwanted activity.
  - Examples of technical corrective controls include patching a system, quarantining a virus, terminating a process, or rebooting a system.
  - Putting an incident response plan into action is an example of an administrative corrective control.

Security Control Functions

- Recovery controls
  - Recovery controls are somewhat like corrective controls, but they are applied in more serious situations to recover from security violations and restore information and information processing resources.
  - Recovery controls may include,
    - disaster recovery and business continuity mechanisms
    - backup systems and data
    - emergency key management arrangements and similar controls.

Security Control Functions

- Compensation controls
  - Compensating controls are intended to be alternative arrangements for other controls when the original controls have failed or cannot be used.
    - When a second set of controls addresses the same threats that are addressed by another set of controls, it acts as a compensating control.

Access Control Models

- The term ‘access control’ refers to “the control of access to system resources after a user’s account credentials and identity have been authenticated and access to the system has been granted”.

Access Control Models

- Access control is used to identify a subject (user/human) and to authorize the subject to access an object (data/resource) based on the required task.
- These controls are used to protect resources from unauthorized access and are put into place to ensure that subjects can only access objects using secure and pre-approved methods.

Access Control Models

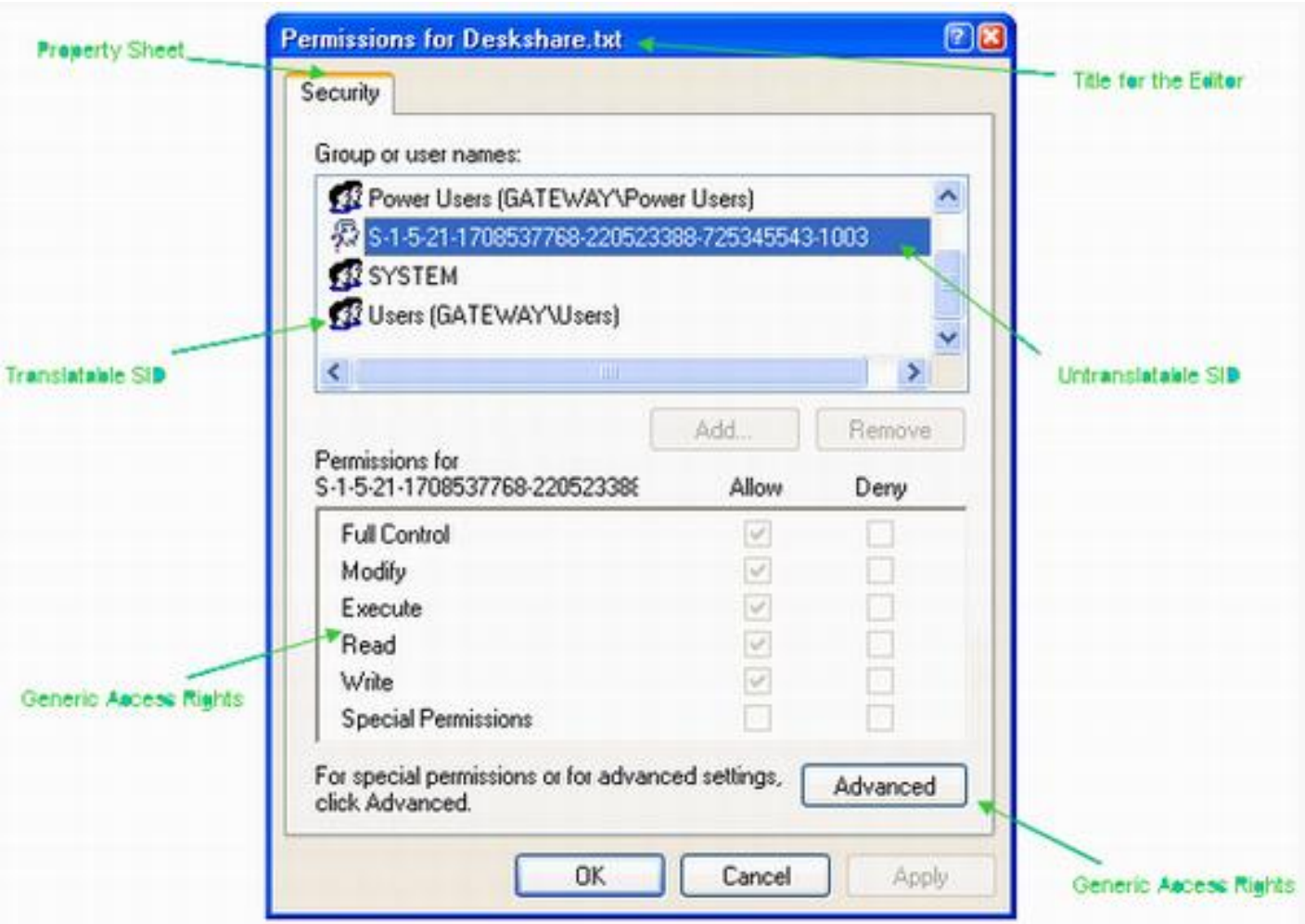
- Logical access control models are the abstract foundations upon which actual access control mechanisms and systems are built. Access control is among the most important concepts in computer security. Access control models define how computers enforce access of subjects (such as users, other Computers, applications and so on) to objects (such as computers, files, directories, applications, servers and devices).

Access Control Models

- Discretionary Access Control Model
- Mandatory Access Control Model
- Role based Access Control Model

Access Control Models

- Discretionary Access Control Model(DAC)



Access Control Models

- Discretionary Access Control(DAC)
  - DAC is a type of access control system that assigns access rights based on rules specified by users. The principle behind DAC is that subjects can determine who has access to their objects.

Access Control Models

- Mandatory Access Control Model(MAC)
  - The design and implementation of MAC is commonly used by the government. It uses a hierarchical approach to control access to files/resources. Under a MAC environment, access to resource objects is controlled by the settings defined by a system administrator.

Access Control Models

- Mandatory Access Control Model(MAC)
  - This means access to resource objects is controlled by the operating system based on what the system administrator configured in the settings. It is not possible for users to change access control of a resource.

Access Control Models

- Mandatory Access Control Model(MAC)
  - Each user account is also assigned classification and category properties.
  - This system provides users access to an object if both properties match. If a user has high classification but is not part of the category of the object, then the user cannot access the object.

Access Control Models

- Mandatory Access Control Model(MAC)

Access Control Models

- Role-Based Access Control (RBAC)
  - RBAC, also known as a non-discretionary access control, is used when system administrators need to assign rights based on organizational roles instead of individual user accounts within an organization.
  - It presents an opportunity for the organization to address the principle of ‘least privilege’. This gives an individual only the access needed to do their job, since access is connected to their job.

Access Control Models

- Role-Based Access Control (RBAC)