Protection and Security

Protection and security

Protection is a mechanism to control access to resources.

Protection mechanisms provide controlled access by limiting the type of access that various users can make.

Security is a measure of confidence that the integrity of a (computer) system relies on.

A security system prevents unauthorized access to a system.

Goals of protection

- Prevent accidental and maliciously destructive behavior.
- Ensure fair and reliable resource usage.
- Provide a mechanism for the enforcement of the policies governing resources use.

Policy: what is to be done.
Mechanism: how something is to be done.

Access control

Domain—a set of <*object,rights*> pairs

Domain structure—access/usage rights associated with particular domains.

E.g.: modern operating systems:
user/kernel mode two domains
UNIX:
each user is a domain, groups of users

Access control matrix represents the policies. Can be implemented as:

– Access control lists (ACL)—row-wise organization
– Capability Lists—column-wise organization

Security

Protection is an internal (within a computer system) problem.

Security includes external environments as well.

Security measures:

- Physical—securing a site from intruders.
- Human—eliminating bribery.

Security violations—unauthorized:

- reading of data
- modification of data
- destruction of data

Authentication

Ability to identify a legitimate user from malicious ones. Based on some combination of three sets of items:

- user possession (a key or a card)
- user knowledge (a user ID or password)
- user attributes (finger print, retina pattern, signature)

Security threats

Fall into four broad categories:

- *Leakage*: the acquisition of information by unauthorized users.
- *Tampering*: the unauthorized alteration of information.
- *Resource stealing*: the unauthorized use of facilities.
- *Vandalism*: interference with the proper operation of a system.

Methods of attack

In order to *violate* a system in the above ways, access to a system is required. Typical attacks include:

- Eavesdropping: to obtain unauthorized copies of messages.
- Masquerading: to send or receive message with unauthorized identity.
- Message tampering: to intercept and alter messages in transit.
- Message replaying: to store messages and send them later.

Infiltration

A simple (direct) method of infiltration to launch such attacks is to guess (legitimate) passwords. Indirect methods of attacks include:

- Virus
- Worm
- Trojan horse
- Trap door

Encryption

A common method of protecting information transmitted over *unreliable* links. Basic encryption mechanism is as follows:

- The information is *encrypt*ed from its initial form (clear text) to an internal form (cipher text).
- The cipher text can be stored or transmitted.
- The receiver *decrypt*s the cipher text back to clear text.

There are two common techniques:

- Secret key
- Public key