Protection

- Protection of resources requires
  - **Access control**: the ability to verify and enforce access rights
  - **Authorization**: the ability to grant and revoke access rights

General Model of Access Control

- Protection is enforced by a **reference monitor**
- A reference monitor records which subject may do what, and decides whether a subject is allowed to have a specific operation carried out
- The reference monitor is called each time an object is invoked
Access Control Matrix

- An access control matrix is used to model the access rights of subjects w.r.t. objects
  - Rows represent subjects and columns represent objects
  - An entry $M[s,o]$ lists which operations subject $s$ can request to be carried out on object $o$
- Efficient ways to implement an access control matrix
  - Each object is associated with an access control list (ACL) represented as a list of subject-rights pairs
    - An ACL corresponds to one column of the access control matrix
  - Each subject is associated with a list of capabilities (i.e. access rights) it has for each object
    - A capabilities list corresponds to one row in the access control matrix

ACL vs. Capabilities

Comparison between ACLs and capabilities for protecting objects. (a) Using an ACL. Authentication of the subject is required. (b) Using capabilities. Authentication is not required.
Implementation of Capabilities in Amoeba

A capability is a 128-bit identifier
- Server port identifies the object’s server
- Object identifies the object at the given server
- Rights specifies the access rights of the holder of the capability
- Check is used to make a capability unforgeable

Amoeba’s Capabilities

When an object is created, its server picks a random check field, turns on all the right bits, and returns this **owner capability** to the client
- Server stores the check field in an internal table

To create a restricted capability
- A client passes a capability and a bit mask for the new rights to the server
- Server creates a new capability (as shown in the figure) and returns it to the client
- The client may send the new capability to another process
Amoeba’s Capabilities (continued)

• To verify a restricted capability, the server
  – XORs the original check with the rights field from the capability
  – passes the result through the one-way function
  – If the result agrees with the check field, the capability is accepted as valid
• To revoke a capability, the server changes the original check field
  – The access is revoked for all holders of the capability

Firewalls

• A firewall is a reference monitor that sits between an organization’s internal network and the outside world, and controls the external access to the organization’s internal network
• Two types of firewalls:
  – Packet-filtering firewalls: filter network packets based on the contents of headers (e.g., source and destination IP address, port number)
  – Application-level firewalls: filter messages based on their contents (e.g., spam filtering email gateways)