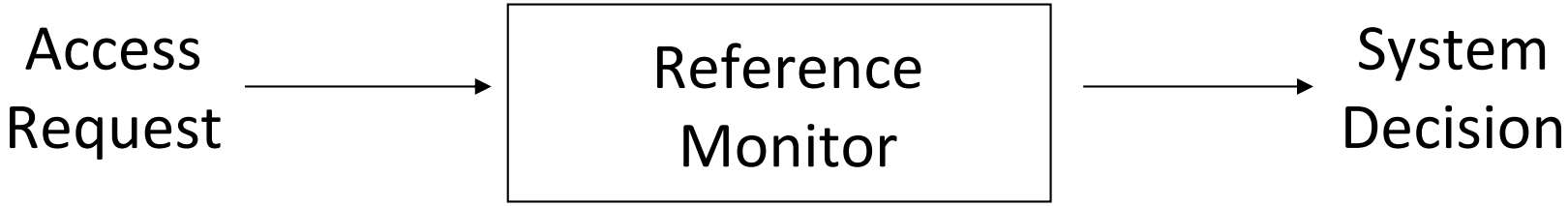
A Schematic View

- A user requests access (*read, write, execute,* …) to a resource (*file, directory, network port*, …) in the computer system

- The *reference monitor*
  - Establishes the validity of the request ….
  - … and returns a decision either granting or denying access to the user

bugejjioseph.com



Simple Analogies

- Consider a paper-based office in which certain documents should only be read by certain individuals

- We could implement security by
  - storing documents in filing cabinets
  - issuing keys to the relevant individuals for the appropriate cabinets

bugejajoseph.com

The Access Control Matrix

- A request can be regarded as a triple (*s*,*o*,*a*)
  - *s* is a subject
  - *o* is an object
  - *a* is an access operation

- A request is granted (by the reference monitor) if
  - *a* belongs to the access matrix entry corresponding to subject *s* and object *o*

bugeiajoseph.com

Access Control Lists

- An ACL corresponds to a column in the access control matrix

- [a.out: (jason, {r,w,x}), (mick, {r,x})]

bugejajoseph.com

Objects / Subjects	trash	a.out	allfiles.txt
jason	{r,w}	{r,w,x}	{r,w}
mick		{r,x}	{r}

- How would a reference monitor that uses ACLs check the validity of the request (jason, a.out, r)?

Access Control Lists

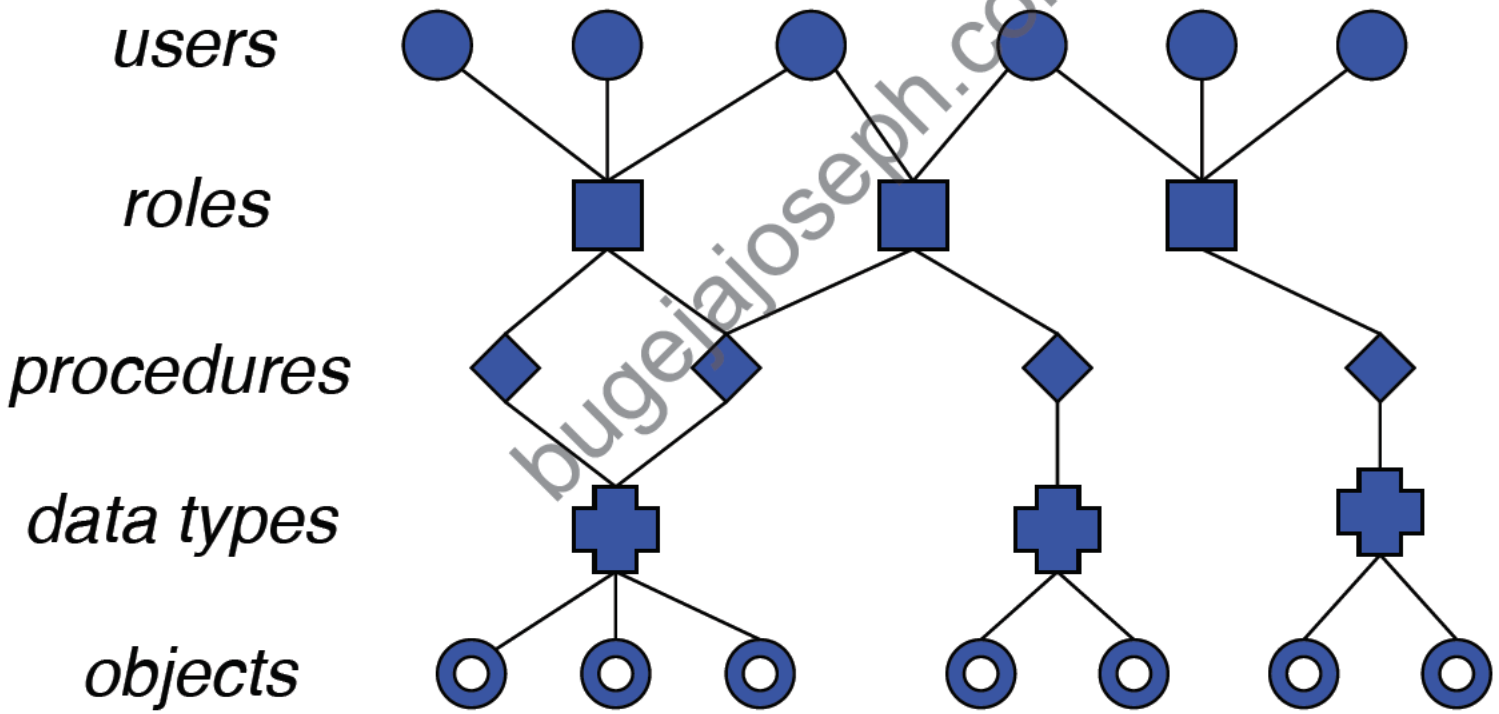
- Access control lists focus on the objects
  - Typically implemented at operating system level
  - Windows and modern UNIX systems use ACLs

- Disadvantage
  - How can we check the access rights of a particular subject efficiently ("before-the-act per-subject review")?

bugejajoseph.com

Intermediate Controls

Intermediate controls for better security management; to deal with complexity, introduce more levels of indirection



bugejajoseph.com

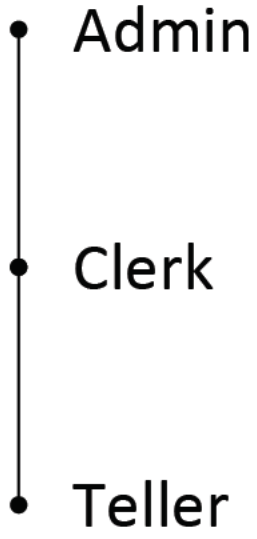
Example

- Objects are bank accounts
- Subjects are bank employees
- The set of bank accounts forms a data type
- We define roles
  - Teller
  - Clerk
  - Administrator
- We define procedures for
  - Crediting accounts (CA)
  - Debiting accounts (DA)
  - Transferring funds between accounts (TF)
  - Creating new accounts (NA)
  - Authorising overdrafts (AO)

bugejajoseph.com

Example

- We assign procedure
  - CA and DA to the Teller role
  - TF to the Clerk role
  - NA and AO to the Administrator role
- We assign all users who are tellers to the Teller role, etc.
- The Administrator role can run all the procedures



Separation of duties

bugeiajoseph.com

Exercises

- What is a reference monitor?
- Mention examples of different access rights used in an information system
- Describe an Access Control Matrix
- What are the disadvantages of Access Control Lists?
- Identify an application that is advantageous to use a capability list

bugejajoseph.com