KF School of Computing and Information Sciences
Florida International University

CNT 4403
Computing and Network Security

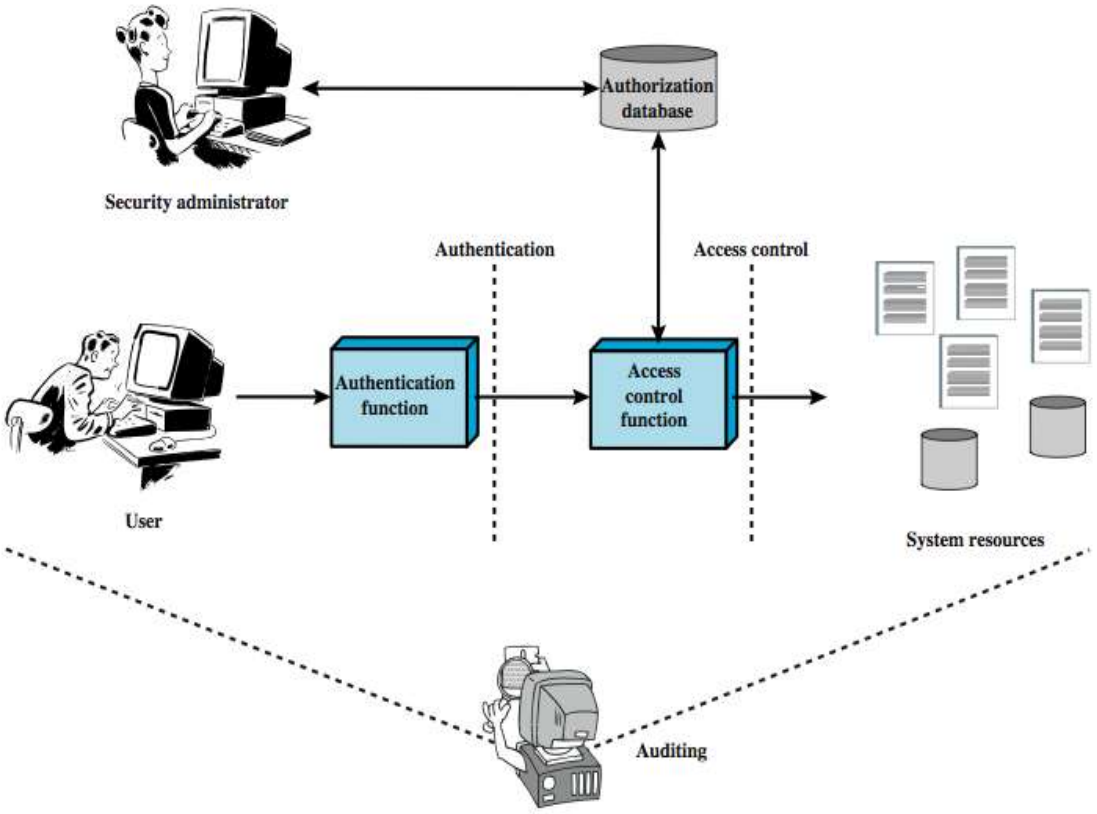
Access Control – Models

Dr. Kemal Akkaya

E-mail: *kakkaya@fiu.edu*

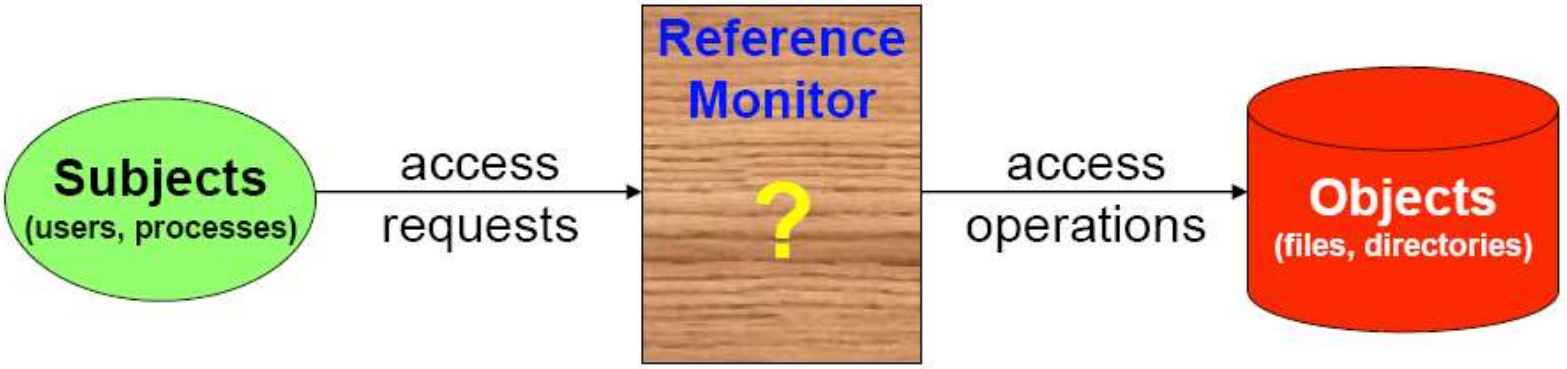
Access Control

- "The prevention of unauthorized users getting access to resources, including the prevention of use of a resource in an unauthorized manner
- Central element of computer security
- Assume have users and groups
  - authenticate to system
  - assigned access rights t certain resources on system



Access Control Elements

- **Subject - entity that can access objects**
  - a process representing user/application
  - often have 3 classes: owner, group, world
- **Object - access controlled resource**
  - e.g. files, directories, records, programs etc
  - number/type depend on environment
- **Access right - way in which subject accesses an object**
  - e.g. read, write, execute, delete, create, search



Access Control Matrix

- Introduced by Butler Lampson in 1971
- Foundation of most access mechanisms used today
- Not suitable for implementation
  - Very sparse
  - Costly in terms of space & processing

Subjects \ Objects	grade.doc	a.out	solution.txt
kfong	{r,w}	{r,w,x}	{r,w}
rchirra		{r,x}	{r}

Access Control Lists (ACLs)

- **The ACL of an object is a list which has:**
  - The subjects who can access to that object
  - The access rights of those subjects
- **Corresponds to a column in Access Control Matrix**
- **Most widely used access control mechanism today**
- **Need to be stored in system memory and queried.**

grade.doc: [(kfong, {r,w})]
a.out: [(kfong, {r,w,x}), (rchirra, {r,x})]
solution.txt: [(kfong, {r,w}), (rchirra, {r})]

Capabilities

- A Capability is an unforgeable ticket that gives a subject certain rights to an object
- Corresponds to a row in the Access Control Matrix

kfong: (grade.doc, {r,w}), (a.out, {r,w,x}), (solution.txt, {r,w})
rchirra: (a.out, {r,x}), (solution.txt, {r})

- A subject who wants to access an object passes an appropriate capability to the system
  - System verifies capability before giving access
- Unlike ACLs, capabilities can be stored in user memory (each user keeps it) and do not need to be searched

Access Control Models

❑ Discretionary access control (DAC):

- ➢ based on the identity of the requestor and access rules (authorizations) stating what requestors are (or are not) allowed to do.
  - ✓ This policy is termed *discretionary* because it is left to the discretion of the object owner
  - ✓ E.g., UNIX permission bits

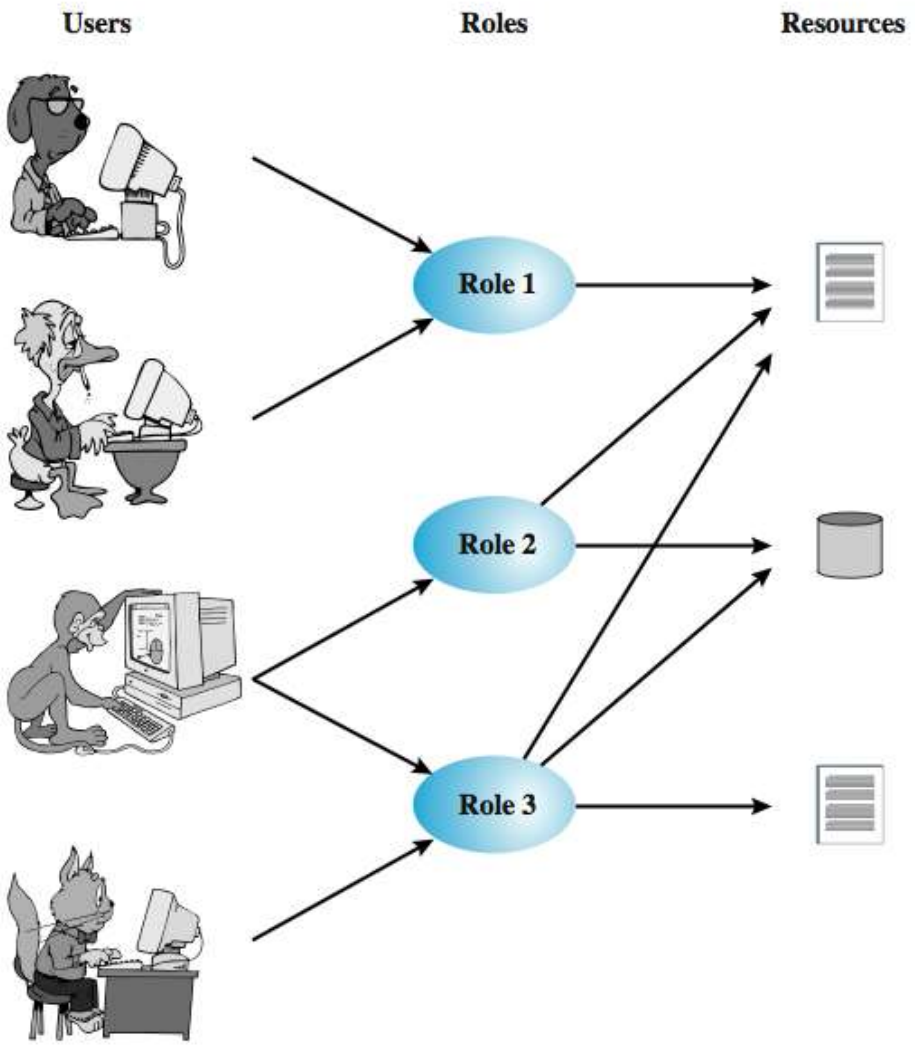
❑ Mandatory access control (MAC):

- ➢ Beyond the control of individual object owner. A central system policy determines which subjects can access which objects.
  - ✓ This policy is termed *mandatory* because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource.
  - ✓ E.g., SELinux

❑ Role-based access control (RBAC):

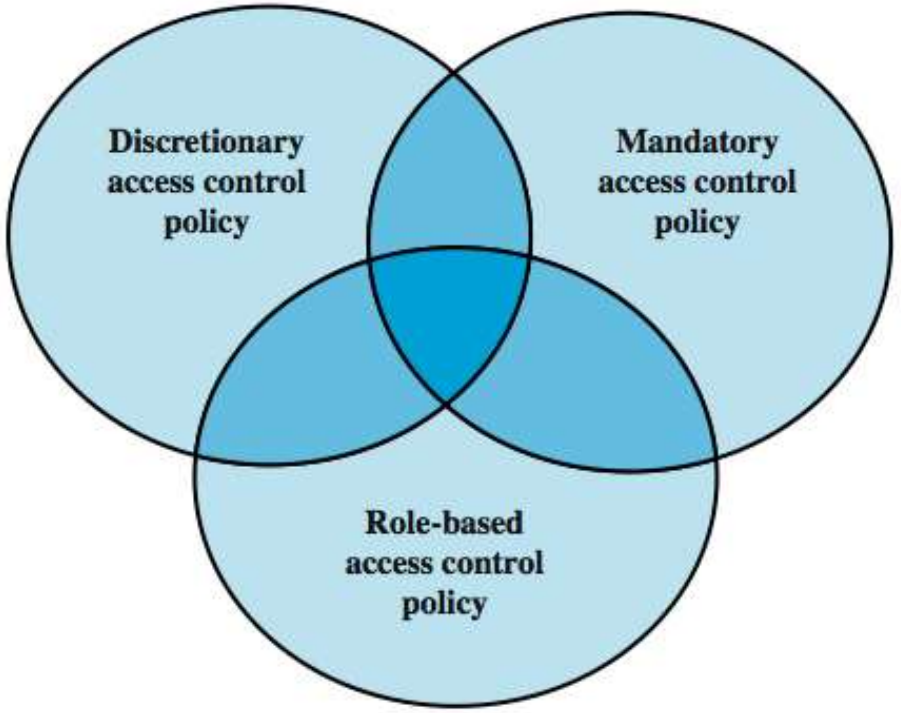
- ➢ based on the roles that users have within the system and rules stating what accesses are allowed to users in given roles.
  - ✓ E.g., Oracle DMBS, MS Windows Active Directory

Role-Based Access Control



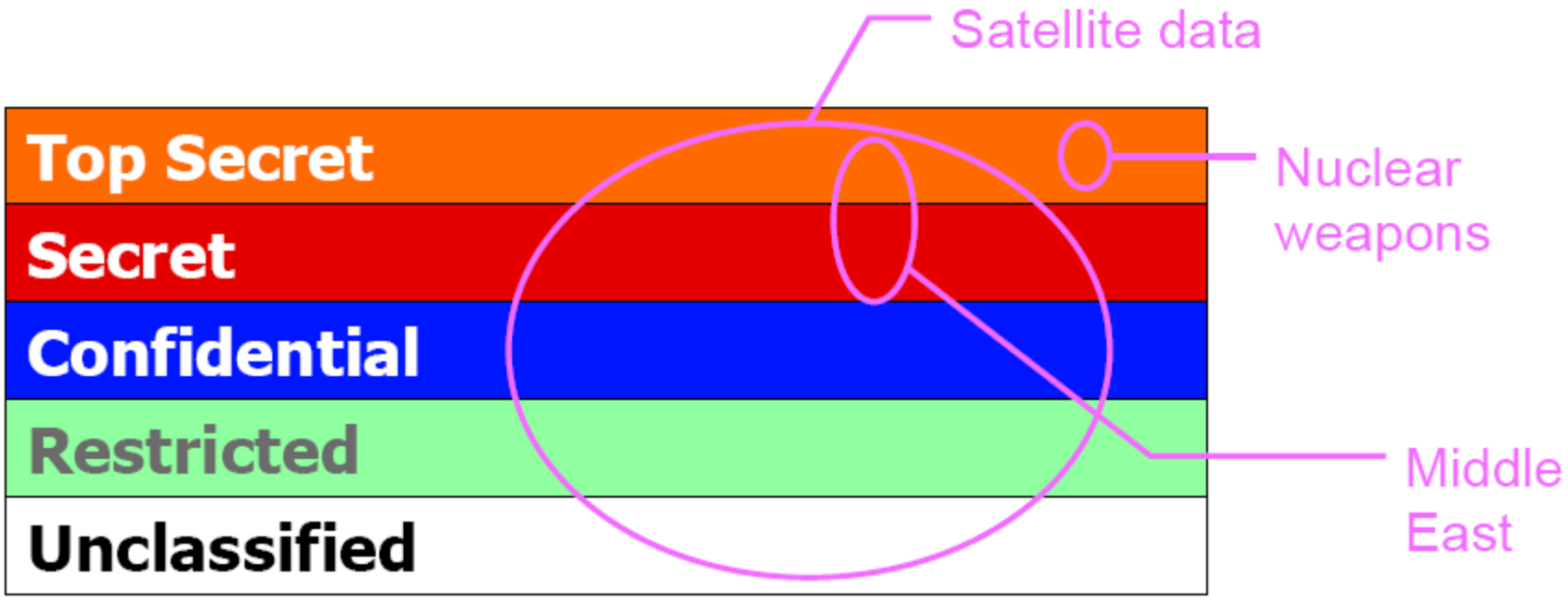
Access Control Models

- DAC is the traditional method of implementing access control.
- MAC is a concept that evolved out of requirements for military information security
- RBAC has become increasingly popular.
- These three models can employ two or even all three of these models to cover different classes of system resources.



Multi-level Security

- Multi-level security (MLS) model is used by the US military and government
- Assigns security level (clearance) to each object and subject



Covert Channels

- **Hidden communications channel that allows transfer of information in a manner that violates the access control policy of the system**
- **A resource is shared by high (Trojan) and low (spy) processes in an MLS**
  - Storage Channel:
    - ✓ Data stored by one process is to be read by the other
  - Timing Channel:
    - ✓ Some system parameter is modulated
- **Covert Channels:**
  - Difficult to detect
  - Can operate for a long time and leak a substantial amount of classified data to uncleared processes
  - Can compromise an otherwise secure system, including one that has been formally verified!