Access Control

Access Control

- Authentication
  - *Who is the user?*
- Authorization
  - *What the user can do?*

Terminology

- Access Control Policies:
  - High level guidelines that determine how accesses are controlled and determined
- Mechanisms:
  - Low level SW/HW functions that implement a policy

Terminology

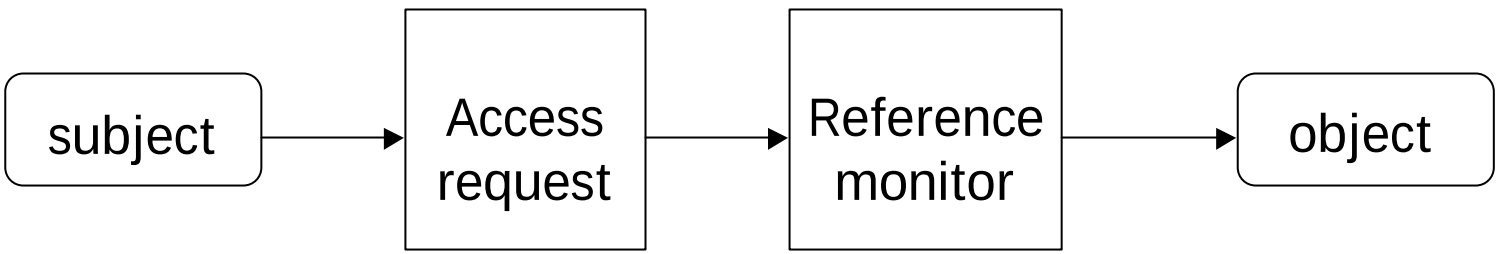
- Subject:
  - Active entities (i.e. process) initiate actions or operations on objects. They can be object as well
- Object:
  - Target of the subject's operations (i.e.files)
- Access rights:
  - Read, write, execute, append, own....

Terminology

- Reference Monitor:
  - has the goal to enforce the policy. It mediates all requested operations by subjects on objects

policies need to be specified and enforced

Access Control Model



Access Control Matrix

- Representation of the access control policy

	file1	file2	file3	file4
John	Read Write Own		R W O	
Alice	R	R W O	W	R
Bob	R W	R		R W O

Access Control List

Stores matrix by columns

file1 $\rightarrow$ John,rwo;Alice,r;Bob,rw

file2 $\rightarrow$ Alice,rwo;Bob,r

file3 $\rightarrow$ John,rwo;Alice,w

file4 $\rightarrow$Alice,r;Bob,rwo

ACL

Pros

- Easy access review with respect to an object
- Easy revocation of accesses to an object

Cons

- Difficult to determine all rights of a subject
- Not very efficient if there is a high turn over of users
- Difficult to revoke all access rights of a subject
- Difficult to delegate access rights

Capabilities

- Stores matrix by columns

John $\rightarrow$ file1,rwo;file3,rwo

Alice $\rightarrow$ file1,r;file2,rwo;file3,w,file4,r

Bob $\rightarrow$ file1,rw;file2,r;file4,rwo

Capabilities

Pros

- Easy access review with respect to a subject
- Possible to delegate access rights to an object

Cons

- Difficult to determine all subjects who can access a particular object
- Difficult to revoke access rights to an object

Groups

- ACL can became very large
- A group is a collection of subjects
- Each group is characterized by a set of access rights
- All subjects member of a group have the access rights of that group.

Es. Unix

```
drwxr-x---  crispo  staff  1024 May 02 11:09  folder1
-rwxrwxr-x  crispo  staff  200192 June 24 17:21  file1
```

Access Control Policies

- Discretionary
- Mandatory

Discretionary Policies

- Subject issues an access request to an object
- If the subject is authorized to do that
  - He is listed in the ACL of the object with the requested access right
  - He has a capability that list the object with the requested access right
- Access is granted

Discretionary Policies

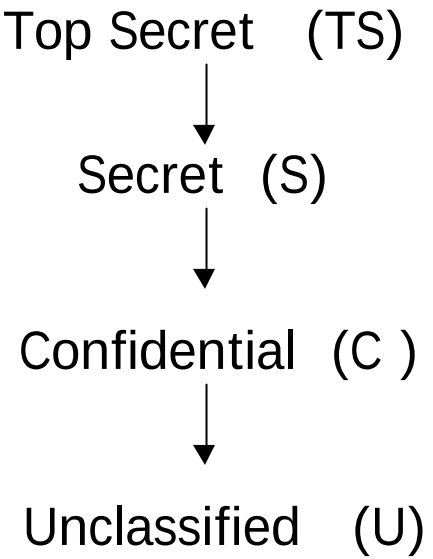
- If the authorization is present the request is served otherwise is rejected
- Advantages
  - Flexibility (e.g. commercial policies)
- Disadvantages
  - Information flow

Mandatory Policies

- A security label is assigned to each subject and each object
- Object's label reflect its security sensitivity
- Subject's label (clearance) is the trustworthiness of the subject not to disclose information he reads

Mandatory Policies

Hierarchical ordered set (i.e., military and government)



Top Secret *dominates* Secret

TS > S > C > U

Mandatory Policies

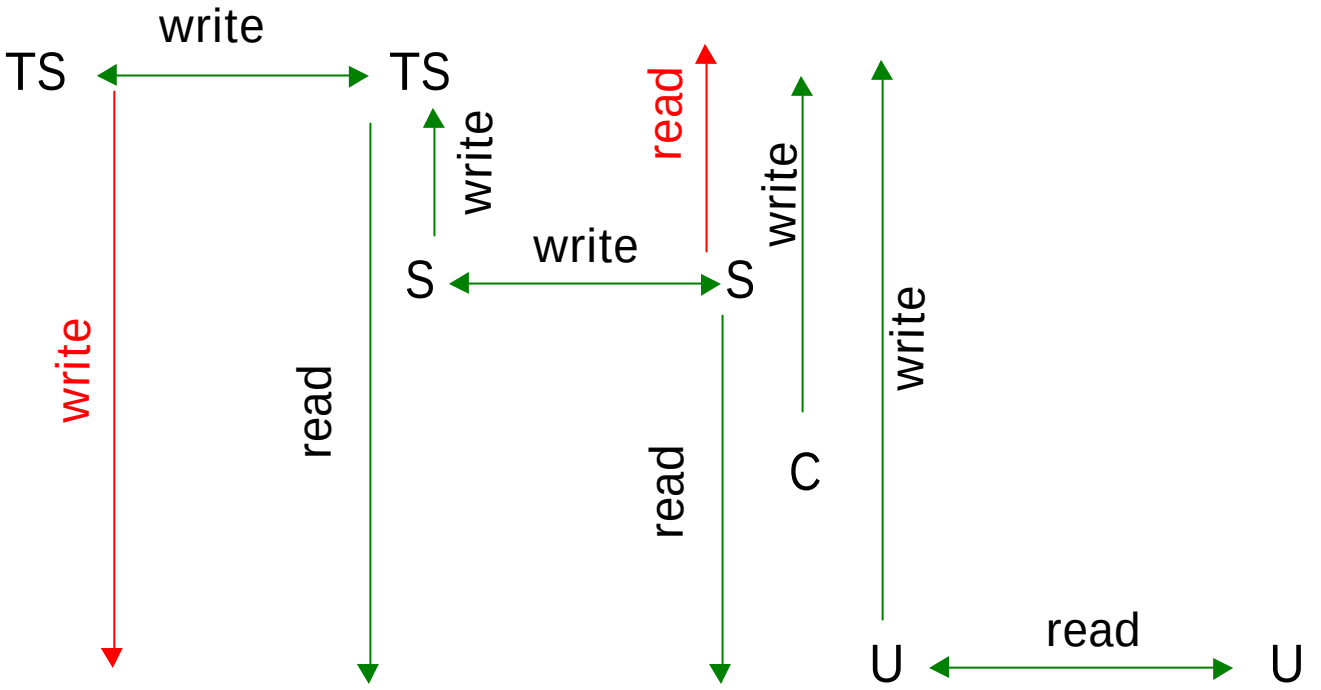
- Subject issues an access request to an object. Access is granted on the basis of the following two rules:

Bell-La Padula model

- *Read down*
  - A subject's clearance must dominate the security level of the object being read
- *Write up*
  - A subject's clearance must be dominated by the security level of the object being written

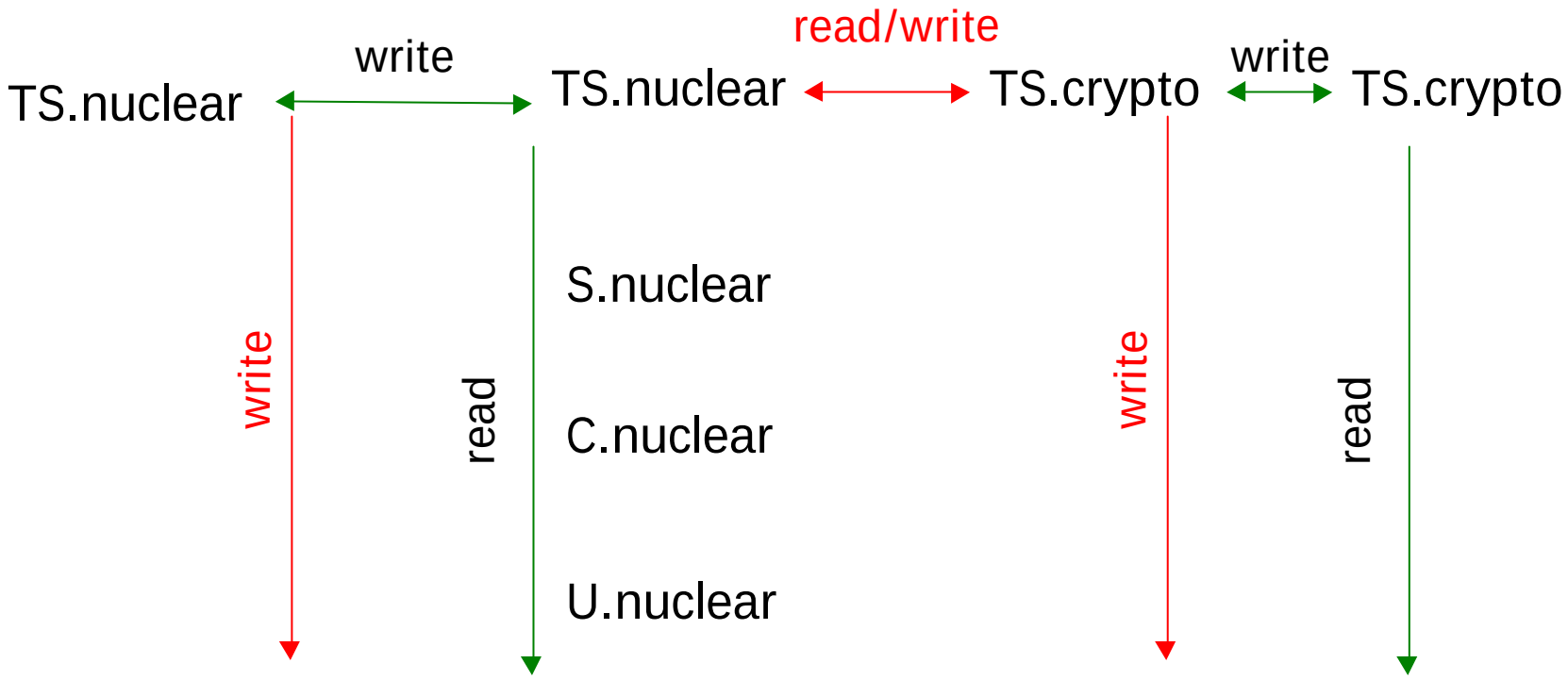
Bell-La Padula model

- Prevent unauthorized information flow
- The model trusts users but not programs



Bell-La Padula model

- Compartments refine labels to provide finer granularity



Bell-La Padula model

TS.nuclear $>$ S.crypto

iff

TS $\geq$ S and nuclear $\supseteq$ crypto

$X.S_1 > Y.S_2$ *iff* $X > Y$ *and* $S_1 \supseteq S_2$

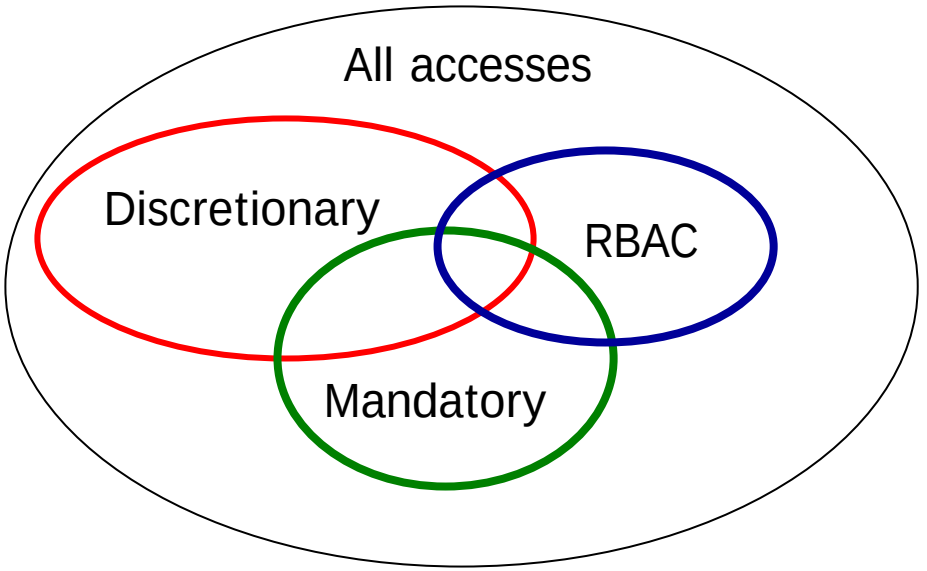
Bell-La Padula model

- Advantages
  - High assurance
  - High value to confidentiality
- Disadvantages
  - Not very flexible
  - Many commercial policies value integrity more than confidentiality

Covert Channel

- Timing channel
- Storage channel

Multiple Access Control Policies



- Intersection applies
- Care to avoid conflicts