Access Control

LECTURE 4

Access Control

Protecting general objects, such as files, tables, access to hardware devices or network connections and other resources.

In general, we want a flexible structure, so that certain users can use a resource in one way (e.g., read-only), others in a different way (e.g., allowing notification) and still others not at all.

Access Control Paradigm

A subject is permitted to access an object in a particular mode, and only such authorized accesses are allowed.

- *Subjects* are human users, often represented by surrogate programs running on behalf of the users.
- *Objects* are things on which an action can be performed: Files, tables, programs, memory objects data fields, network connections and processors.
- *Access modes* are many controllable actions of subjects on objects, including, but not limited to, read, write, modify, delete, execute and so on.

Access Policies

Access control is a mechanical process, easily implemented by a table and computer process: A given subject either can or cannot access a particular object in a specified way.

Before trying to implement access control, an organization needs to take the time to develop a higher-level security policy, which will then drive all the access control rules.

Access Policies

- *Effective Policy Implementation:*
  - *Check every access.*
  - *Enforce least privilege*: access to the fewest resources necessary to complete some task.
  - *Verify acceptable usage*.
- Tracking
- Granularity
- Access Log
- Limited Privilege

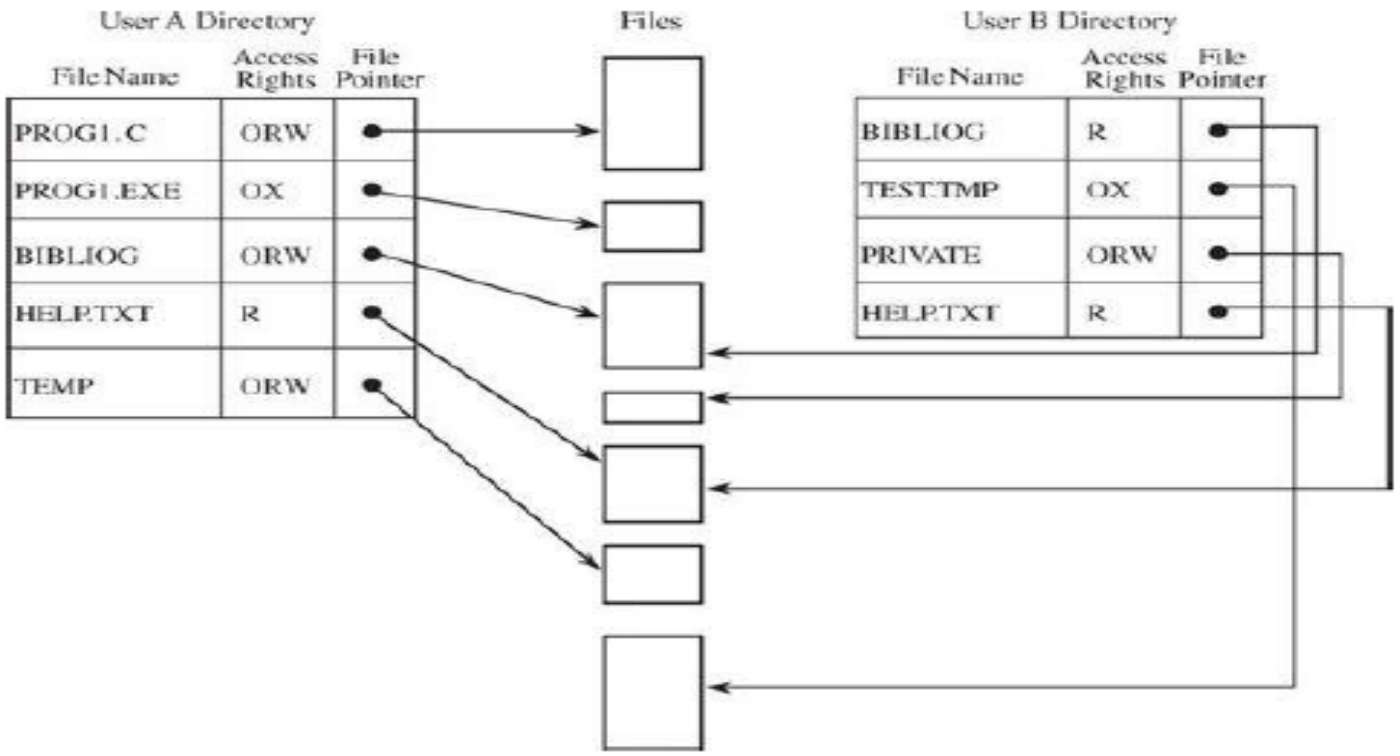
Implementing Access Control

Access control is often performed by the operating system.

- Reference Monitor: access control that is always invoked, tamperproof, and verifiable.

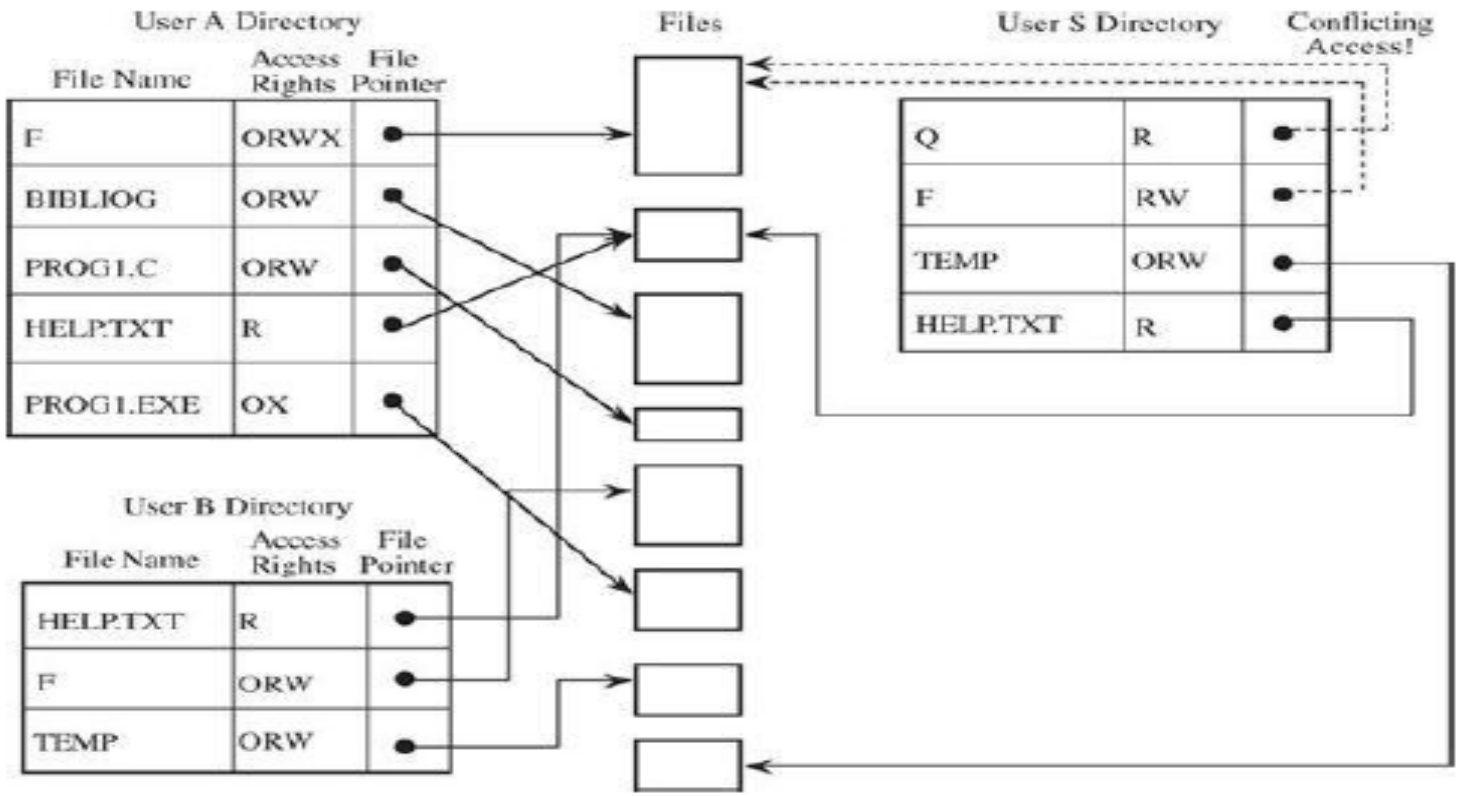
- A reference monitor is a notion, not a tool you can buy to plug into a port. It could be embedded in a application (to control the application's objects), part of the operating system (for system-managed objects) or part of an appliance.

Access Control Directory



Directory Access Rights

Access Control Directory



Ambiguous Access Rights

Access Control Matrix

objects

subjects

	File A	Printer	System Clock
User W	Read Write Own	Write	Read
Admin		Write Control	Control

Access Control Matrix

Access Control Matrix

	Bibliog	Temp	F	Help .txt	C_ Comp	Linker	Clock	Printer
USER A	ORW	ORW	ORW	R	X	X	R	W
USER B	R	—	—	R	X	X	R	W
USER S	RW	—	R	R	X	X	R	W
USER T	—	—	R	X	X	X	R	W
SYS MGR	—	—	—	RW	OX	OX	ORW	O
USER SVCS	—	—	—	O	X	X	R	W

Access Control Matrix

Access Control Matrix

Subject	Object	Right
USER A	Bibliog	ORW
USER B	Bibliog	R
USER S	Bibliog	RW
USER A	Temp	ORW
USER A	F	ORW
USER S	F	R
etc.		

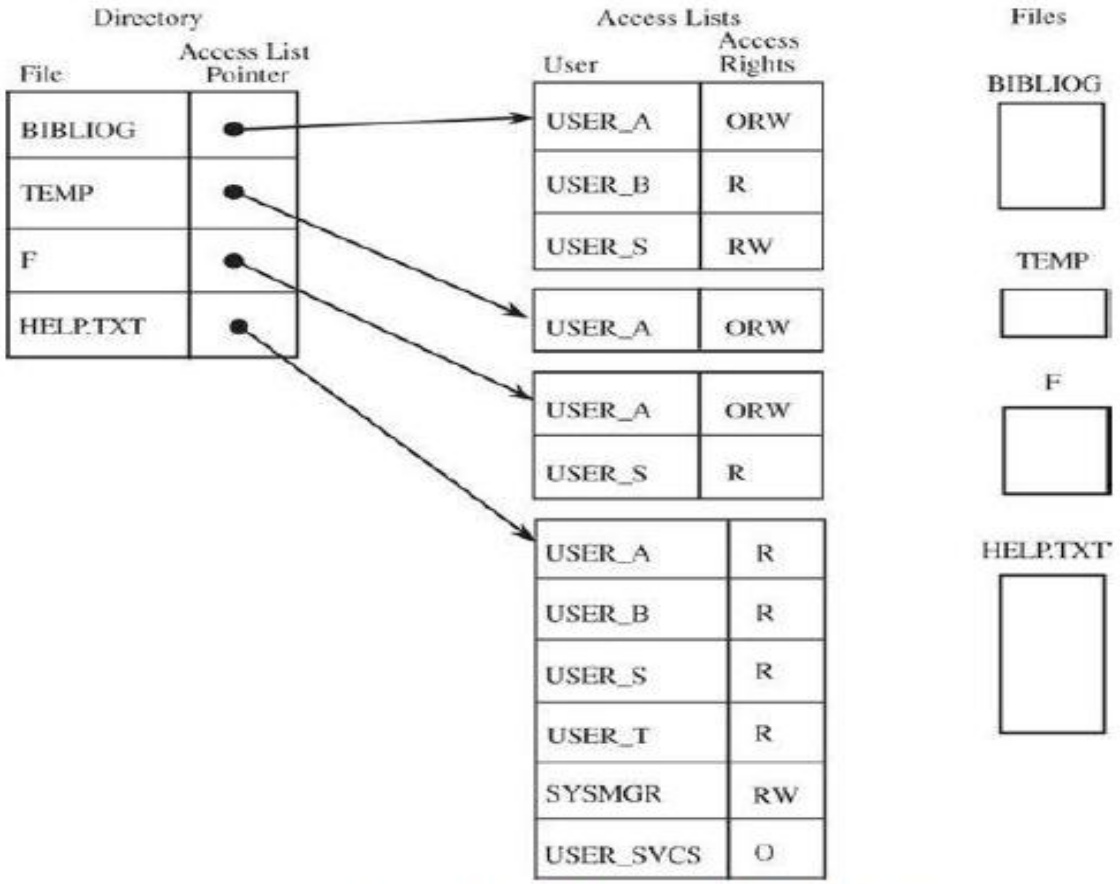
List of Access Control Triples

Access Control List

	File A	Printer	System Clock
User W	Read Write Own	Write	Read
Admin		Write Control	Control

Access Control List

Access Control List



Access Control List with Two Subjects

Privilege List

	File A	Printer	System Clock
User W	Read Write Own	Write	Read
Admin		Write Control	Control

Privilege Control List

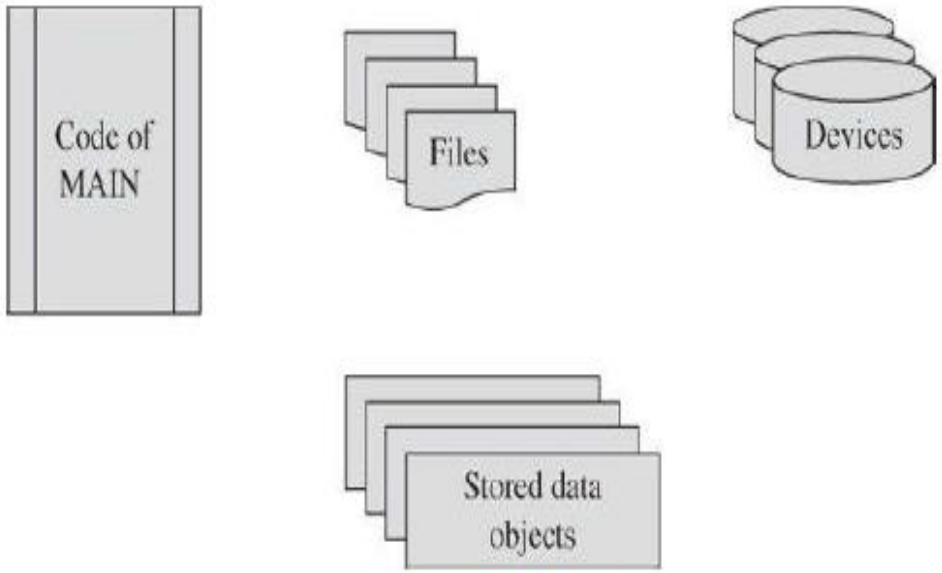
Capability

Capability: Single- or multi-use ticket to access an object or service.

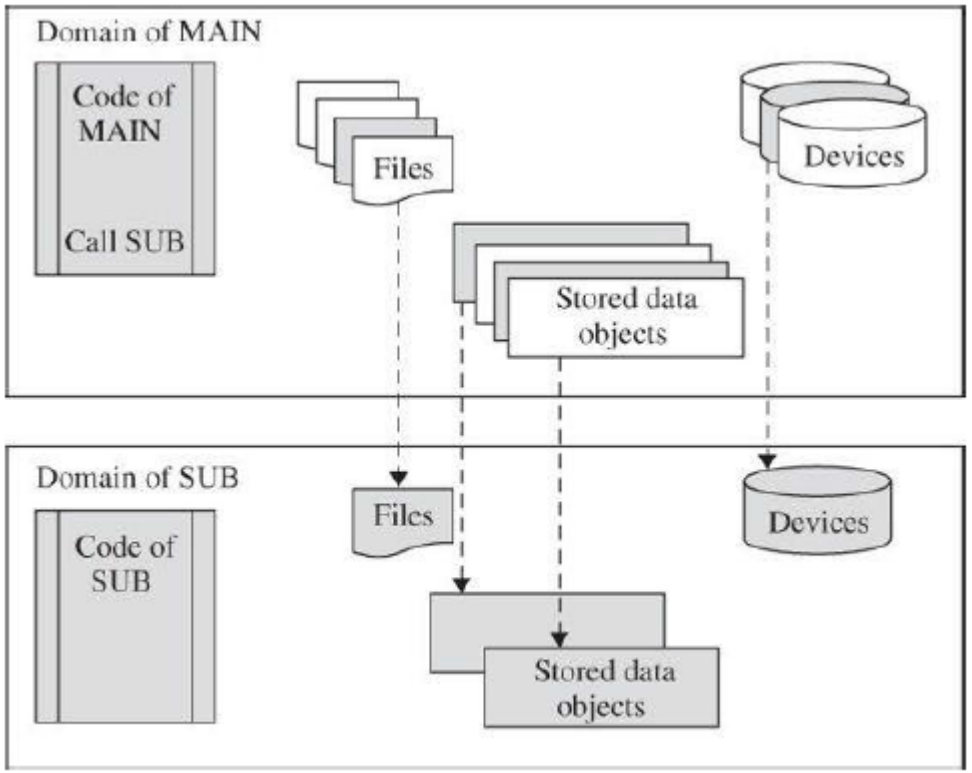
	File A	Printer	System Clock
User W	Read Write Own	Write	Read
Admin		Write Control	Control

Capability

Capability



Example of a Domain



Passing Objects to a Domain