

CS241 System Programming Protection Mechanisms

Klara Nahrstedt

Lecture 27

3/31/2006



Content

- Protection Domains
- Access Control
- Capabilities
- Covert Channels

Administrative

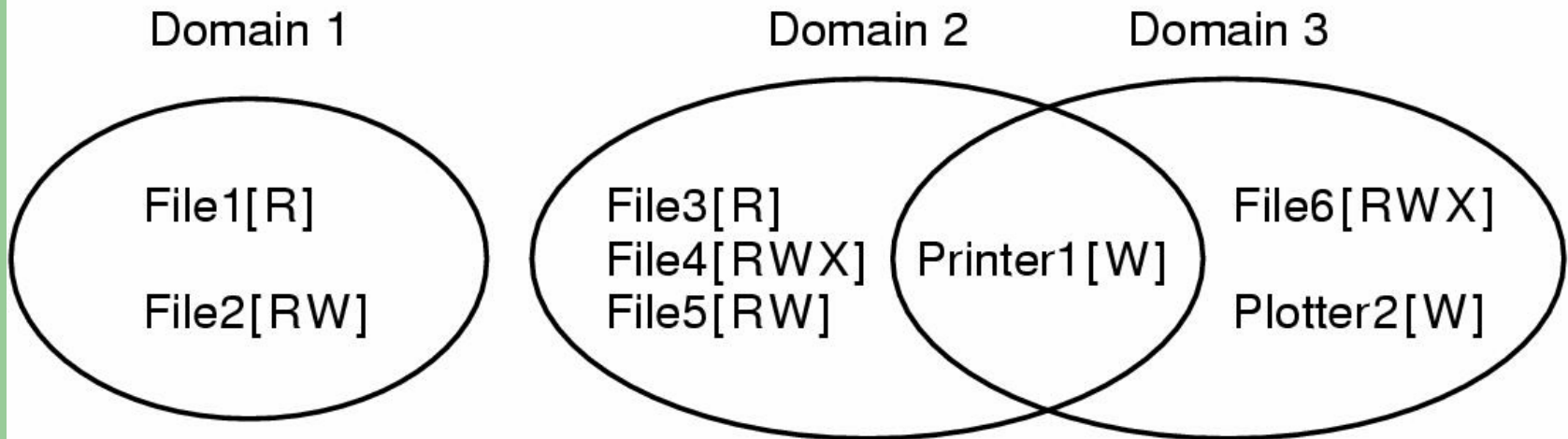
- MP3 is posted, due April 3, 2006
- Quiz 7 is March 31, 2006
- Material covered in Quiz 7
 - R&R Chapter 4 and Chapter 5
 - Tanenbaum Chapter 5.3

Protection Domain

- A computer system is a set of processes and objects
- Processes and objects have unique names
- Objects are abstract data types with well-defined operations
- A process operates within a protection domain
- A protection domain specifies the resources a process may access and the types of operations that may be invoked on the objects.
- **The Principle of Least Privilege *Need to know*: The protection domain of a process should be as small as possible consistent with the need of that process to accomplish its assigned task.**

Protection Mechanisms

Protection Domains



Examples of three protection domains

Protection Matrix

		Object							
		File1	File2	File3	File4	File5	File6	Printer1	Plotter2
Domain	1	Read	Read Write						
	2			Read	Read Write Execute	Read Write		Write	
	3						Read Write Execute	Write	Write

Protection Matrix with Domains as Objects

		Object										
		File1	File2	File3	File4	File5	File6	Printer1	Plotter2	Domain1	Domain2	Domain3
main	1	Read	Read Write								Enter	
	2			Read	Read Write Execute	Read Write		Write				
	3						Read Write Execute	Write	Write			

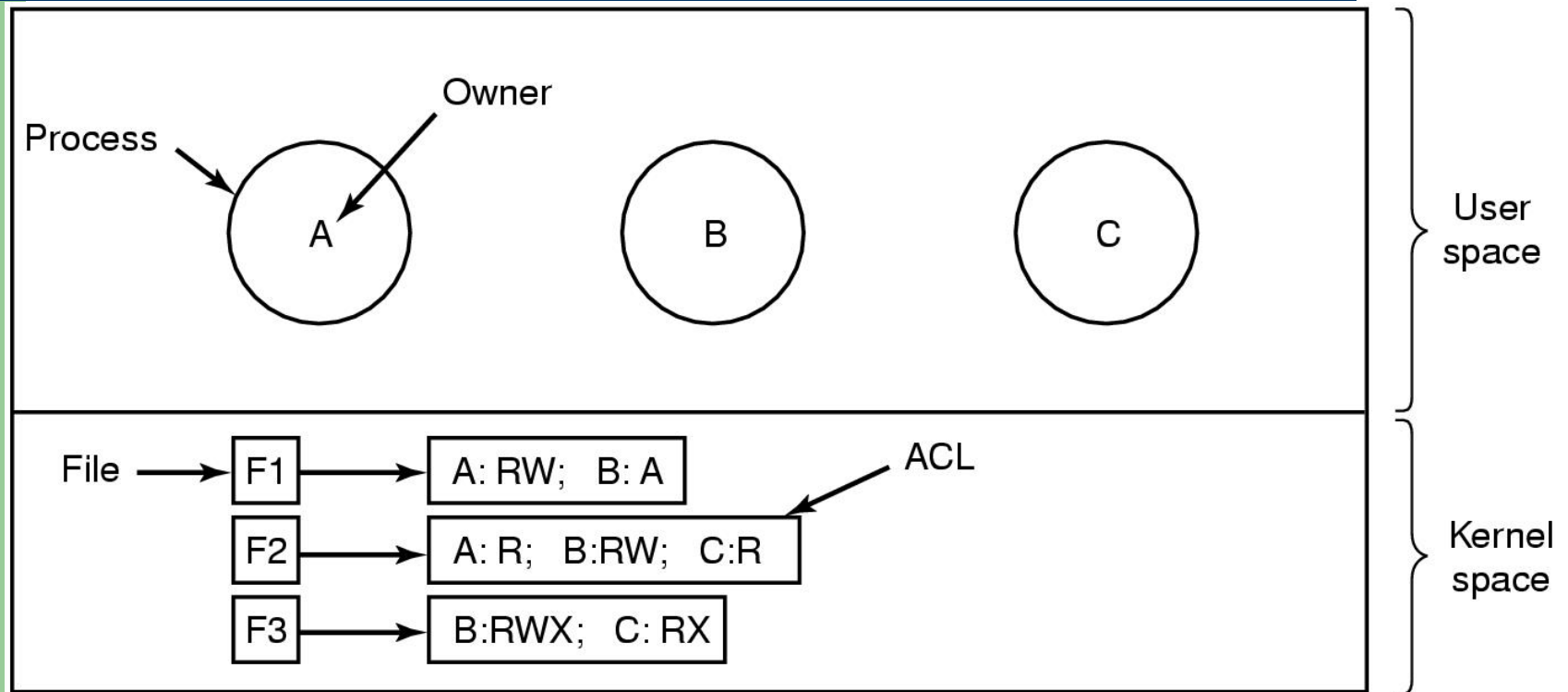
Implementation of Protection Matrix

- **Global Table**
- Table may be Sparse
- Table may be too large to store in main memory (use virtual memory - overhead)
- Objects that may be accessed from every Domain need to be entered in every row
- Needs a searching operation
- In parallel or distributed system, access to table may be bottleneck

Access Lists

- Each **column** in the protection matrix is implemented as an **access list** for one Object.
- Empty entries in Protection Matrix can be discarded.
- Storage for access lists is proportional to the number of Objects
- It is easy for the owner of the Object to grant access to another Domain or revoke access.
- It is easy to determine which processes can access an object.
- However, **all processes can find out that the Object exists.**
- ACL entries can be for individual users or for a group of users.

Access Control Lists

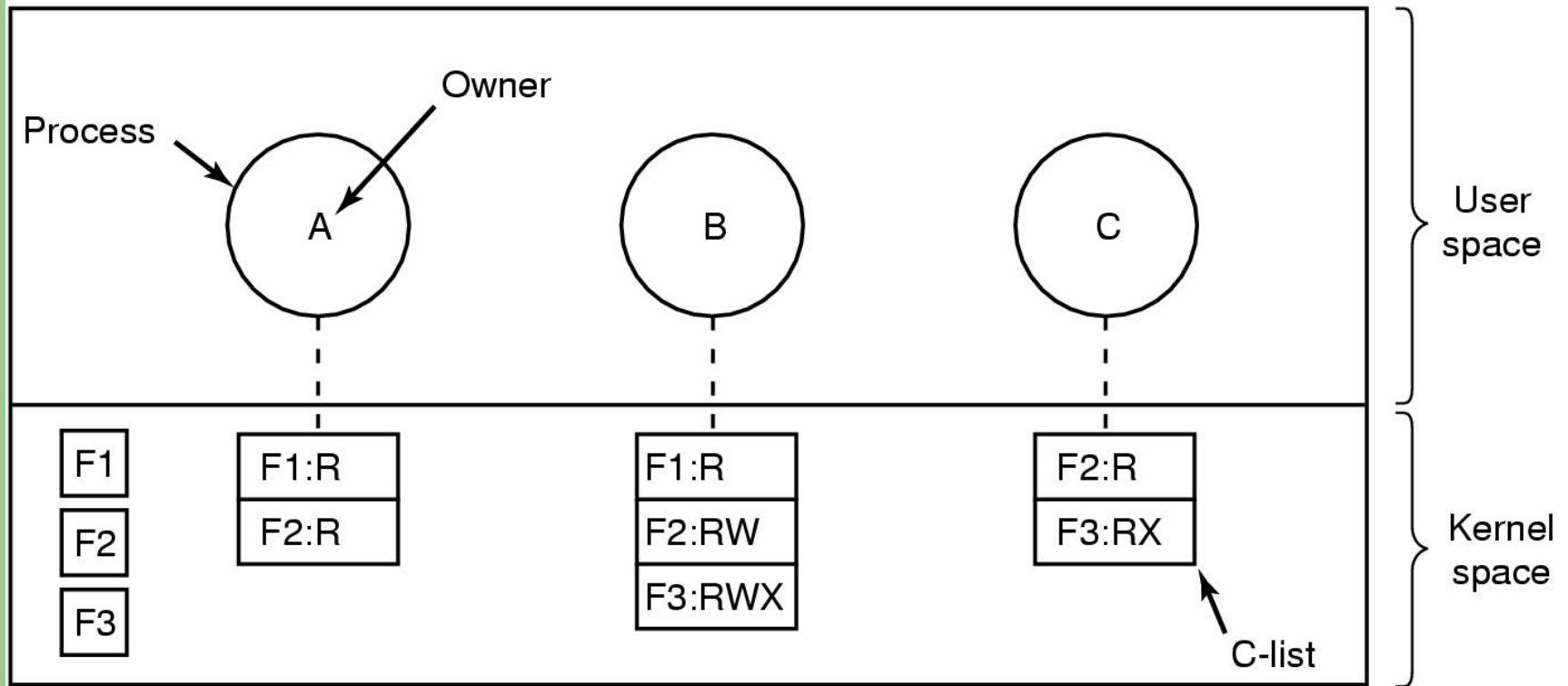


Use of access control lists - managed file access

Capability Lists / C-Lists

- Each **row** in the access matrix is implemented as a capability list for each Domain.
- Empty entries in Access Matrix can be discarded.
- Rather than search, a reference to an object can be treated as an index operation into the capability list.
- A capability is then just a "protected pointer".

Capabilities



Each process has a capability list

Capability Implementations

- UNIX File System

- Each entry in the per process open file descriptor table is a capability.
- It is protected and can only be changed by the kernel.
- Having an open file descriptor permits access.
- This example shows how access lists can be used to achieve simple management of protection and capabilities used to provide efficient access methods.

Discussion

- Tradeoff between Access-list and capability list
 - Give an example for which an access-list should be used
 - Give an example for which a capability-list should be used
- Hints:
 - In what cases, access-list takes more space
 - Which one is easier to delete an object?
 - Which one is easier to delete a domain?
 - Access-list is faster for what operations? Similarly, capability-list is faster for what operations?

Summary

- Access Control using lists and capabilities in File Systems is very important
- Lampson showed that protection matrix may not be sufficient and covert channels may exist, especially if parties collude