CISC 7310X
C14: OS Security: A Few Concepts
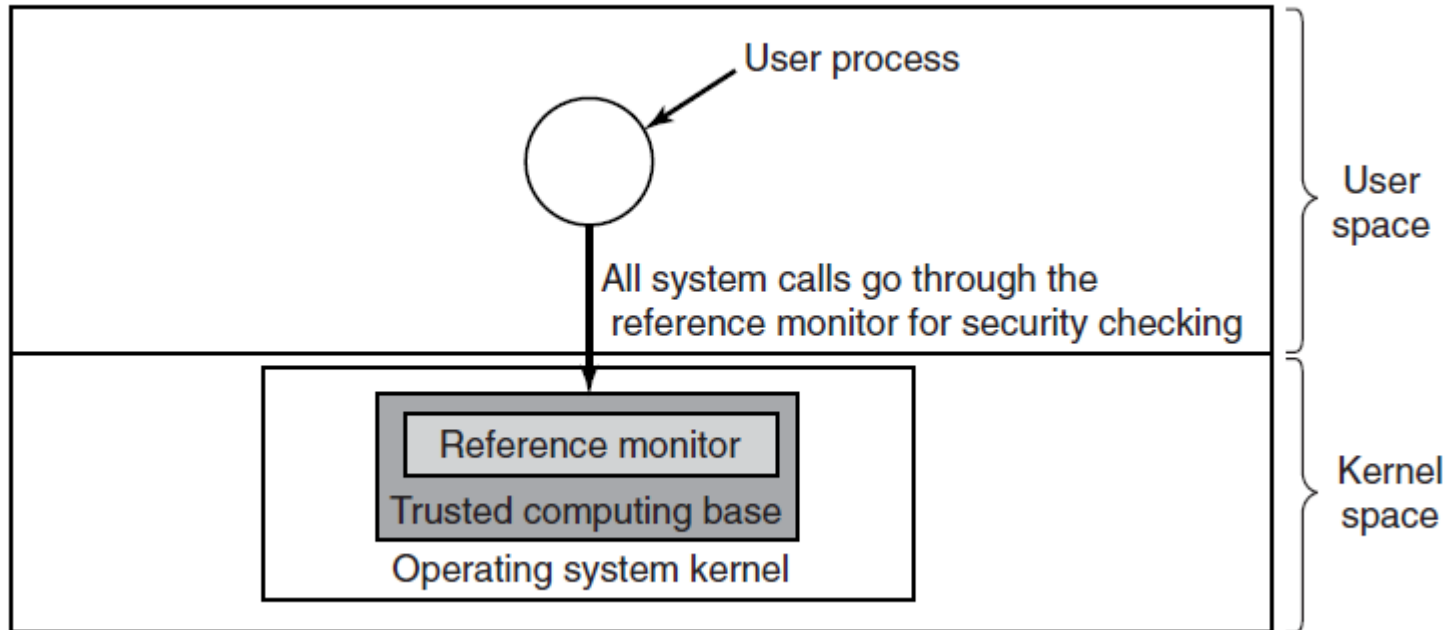
Hui Chen

Department of Computer & Information Science
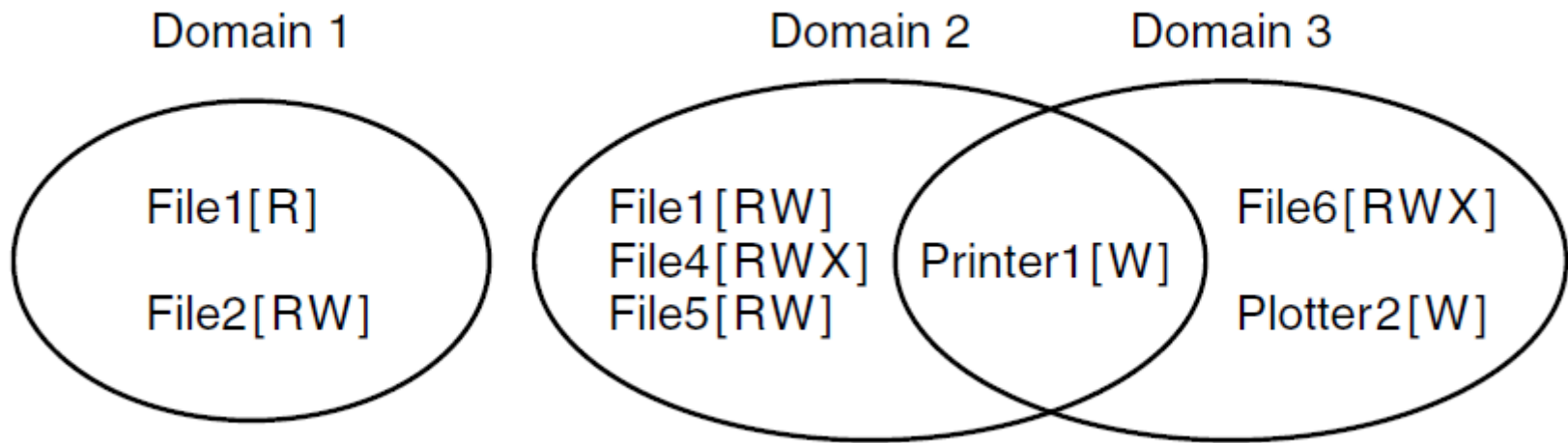
CUNY Brooklyn College

Goals and Threats

- Goals
  - Confidentiality, integrity, availability
  - Additionally,
    - Authenticity, accountability, nonrepudiability, privacy, …

- Threats
  - Exposure of data, tempering with data, denial of service, …

Trusted Computer Base

- [Figure 9-2 in Tanenbaum & Bos, 2014]

CUNY | Brooklyn College

Protection Domains

Domain 1	Domain 2	Domain 3

File1[R]

File2[RW]

File1[RW]
File4[RWX]
File5[RW]

Printer1[W]

File6[RWX]

Plotter2[W]

- [Figure 9-3 in Tanenbaum & Bos, 2014]

Access Control Matrix

- Or protection matrix

	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

Object

- [Figure 9-3 in Tanenbaum & Bos, 2014]
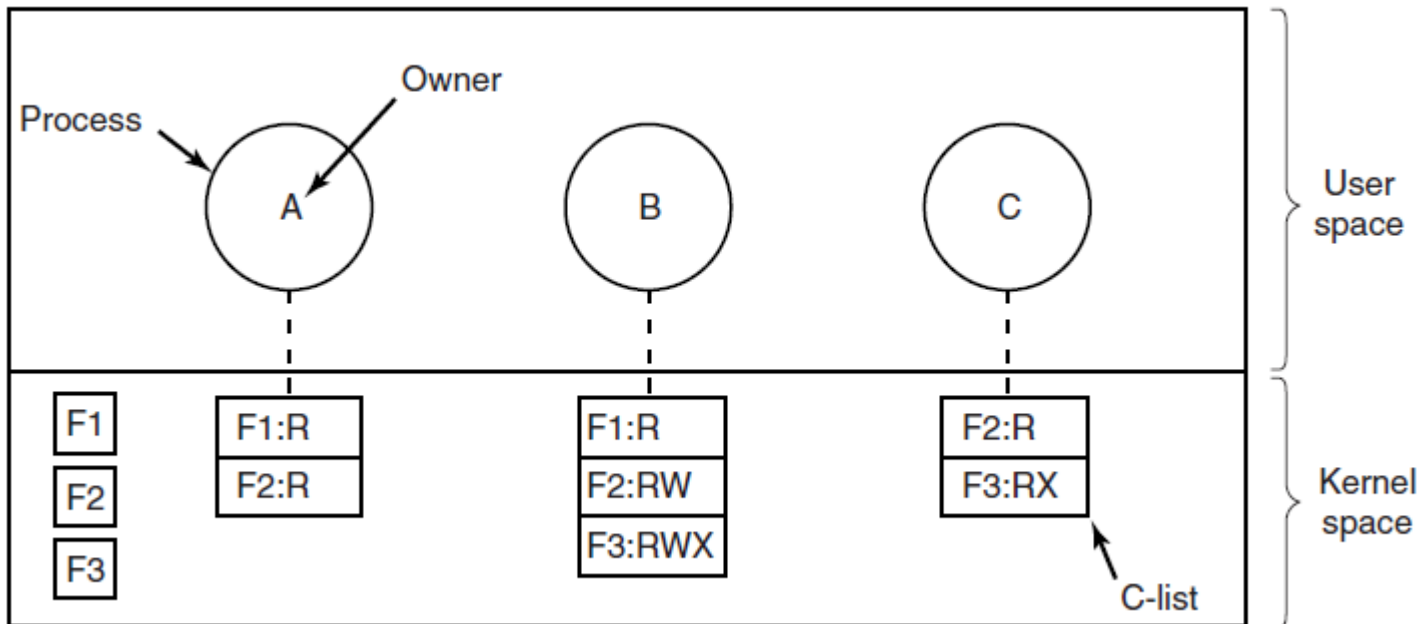
Access Control List

• From matrix to list
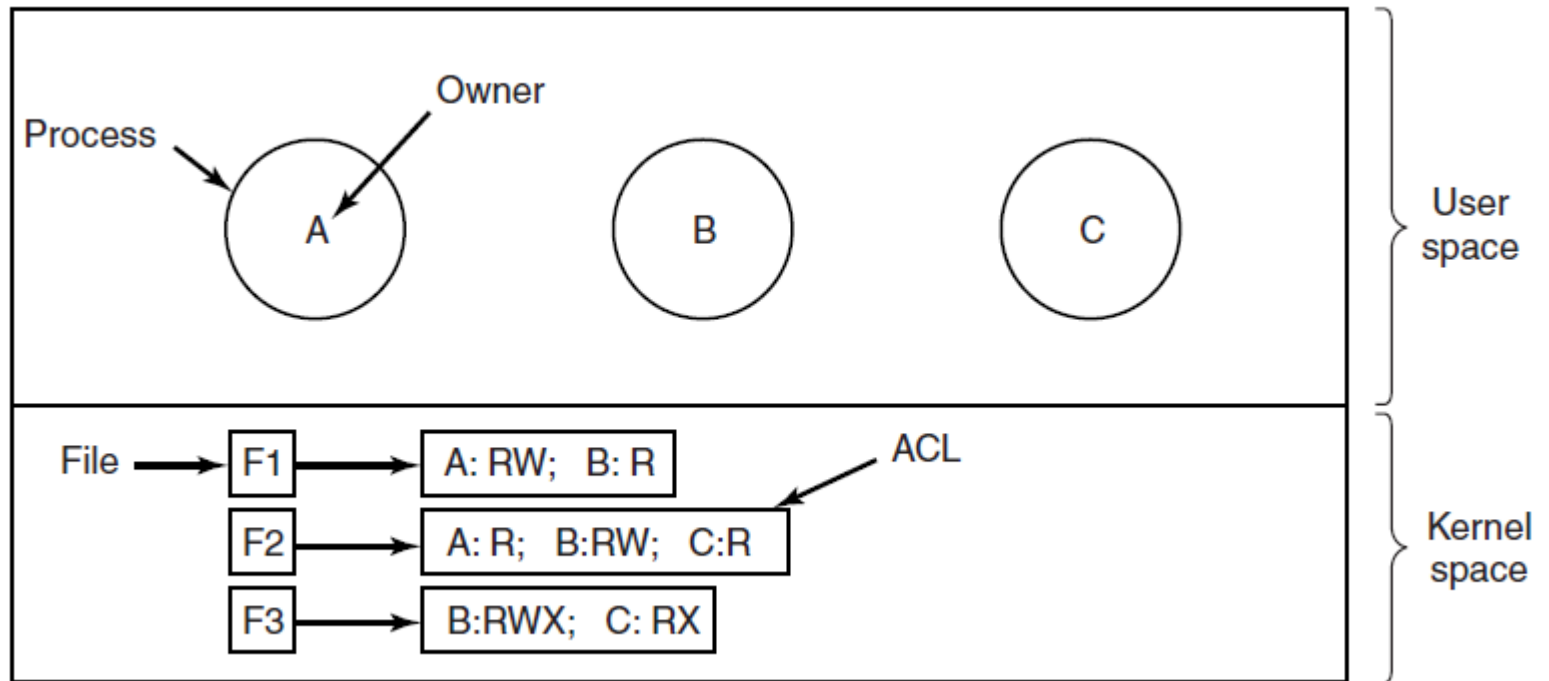
• [Figure 9-3 in Tanenbaum & Bos, 2014]

Capabilities

- From matrix to list

- [Figure 9-8 in Tanenbaum & Bos, 2014]

Formal Model

- Authorized and unauthorized states

Objects

	Compiler	Mailbox 7	Secret
Eric	Read Execute		
Henry	Read Execute	Read Write	
Robert	Read Execute		Read Write

(a)

Objects

	Compiler	Mailbox 7	Secret
Eric	Read Execute		
Henry	Read Execute	Read Write	
Robert	Read Execute	Read	Read Write

(b)

- [Figure 9-10 in Tanenbaum & Bos, 2014]

Questions

- A few concepts in security