Prof. Dr. Carsten Vogt
Exercises „Operating Systems and Distributed Systems 2“
2019/20

Technology
Arts Sciences
TH Köln

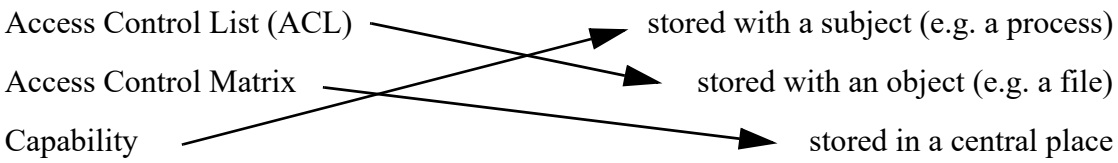
Access Control – Solution

Exercise 1: Techniques for Access Control

- Draw three arrows from the terms on the left to the corresponding explanations on the right:

Access Control List (ACL)	stored with a subject (e.g. a process)
Access Control Matrix	stored with an object (e.g. a file)
Capability	stored in a central place

Solution:



Exercise 2: Rights Management in a Pipelining System

- Given: A processing system with two stages
  - Process P_1
    - reads data from an input file INPUT
    - processes the data by executing the program in the program file $PROG_1$
    - writes intermediate results into the file INTERMEDIATE
  - Process P_2
    - reads data from the file INTERMEDIATE
    - processes the data by executing the program in the program file $PROG_2$
    - writes the final results into the file OUTPUT
- Questions:
  - What are the subjects, what are the objects in this system?

  Solution: Subjects: P_1, P_2 ; objects: INPUT, $PROG_1$, INTERMEDIATE, $PROG_2$, OUTPUT

  - Which operations can be executed on the objects in principle?

  Solution: read (R), write (W), execute (X)

  - What access rights must the subjects have for the objects ...
    - ... specified by an access control matrix?

    Solution:

	INPUT	$PROG_1$	INTER-MEDIATE	$PROG_2$	OUTPUT
P_1	R	X	W	-	-
P_2	--	-	R	X	W

    - ... specified by access control lists?

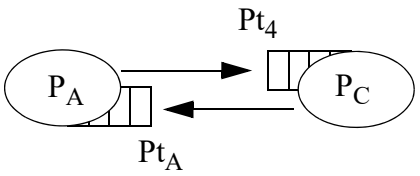
    Solution:
    INPUT: (P_1,R)
    $PROG_1$: (P_1,X)
    INTERMEDIATE: (P_1,W), (P_2,R)
    $PROG_2$: (P_2,X)
    OUTPUT: (P_2,W)

    - ... specified by capabilities?

    Solution:
    P_1: (INPUT, R), ($PROG_1$, X), (INTERMEDIATE, W)
    P_2: (INTERMEDIATE, R), ($PROG_2$, X), (OUTPUT, W)

Exercise 3: Rights Management in a Client-Server System

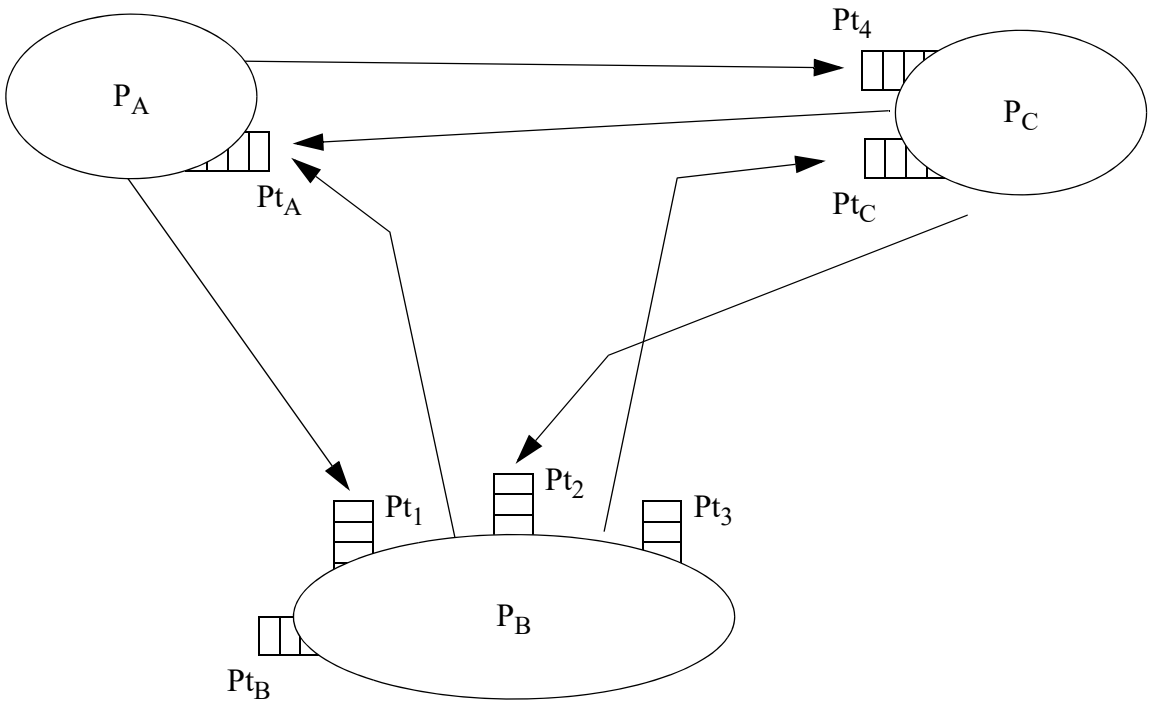
- Given: A client-server system of processes. The processes offer and use services
  - Processes P_A, P_B, P_C
  - Services:
    - P_B offers the services S_1, S_2, S_3.
    - P_C offers the service S_4.
    - P_A uses the services S_1 and S_4.
    - P_C uses the service S_2.
  - Ports:
    - For each service S_i: One request port Pt_i
      - All requests for service S_i are sent to port Pt_i.
    - For each process P_X: One response port Pt_X
      - All responses to process P_X are sent to port Pt_X
        (no matter which of the servers is sending the response)
    - Remember (from chapter 5, foils 6 and 7):
      A port is a mailbox to which multiple processes may write data but from which only one process may read data – the process to which the port is attached.
      Ports are e.g. used in client-server systems to transmit the clients' requests and the servers' responses.
  - Diagram showing a part of the system:



Explanation:
P_C offers S_4 → Pt_4 is attached to P_C
P_A uses S_4 → P_A sends messages to Pt_4
P_A receives replies → Pt_A is attached to P_A
P_C replies to P_A → P_C sends messages to Pt_A

- Do the following:
  - Complete the diagram.

  Solution:



    - Note: The arrows (representing the messages) go into ports but have their origins directly in processes, not in ports!
  - Define the security model:
    - Which are the subjects, which are the objects?

    Solution: subjects P_A, P_B, P_C; objects Pt_1, Pt_2, Pt_3, Pt_4, Pt_A, Pt_B *(Pt_B is not really required here)*, Pt_C

    - Which operations can be executed on the objects in principle?

    Solution: read, write
  - Give the capability lists of the subjects.

  Solution:

    - P_A: (Pt_A,R), (Pt_1,W), (Pt_4,W)
    - P_B: (Pt_B,R), (Pt_1,R), (Pt_2,R), (Pt_3,R), (Pt_A,W), (Pt_C,W)
    - P_C: (Pt_C,R), (Pt_4,R), (Pt_2,W), (Pt_A,W)