ACCESS CONTROL LAST
Lecture 5a

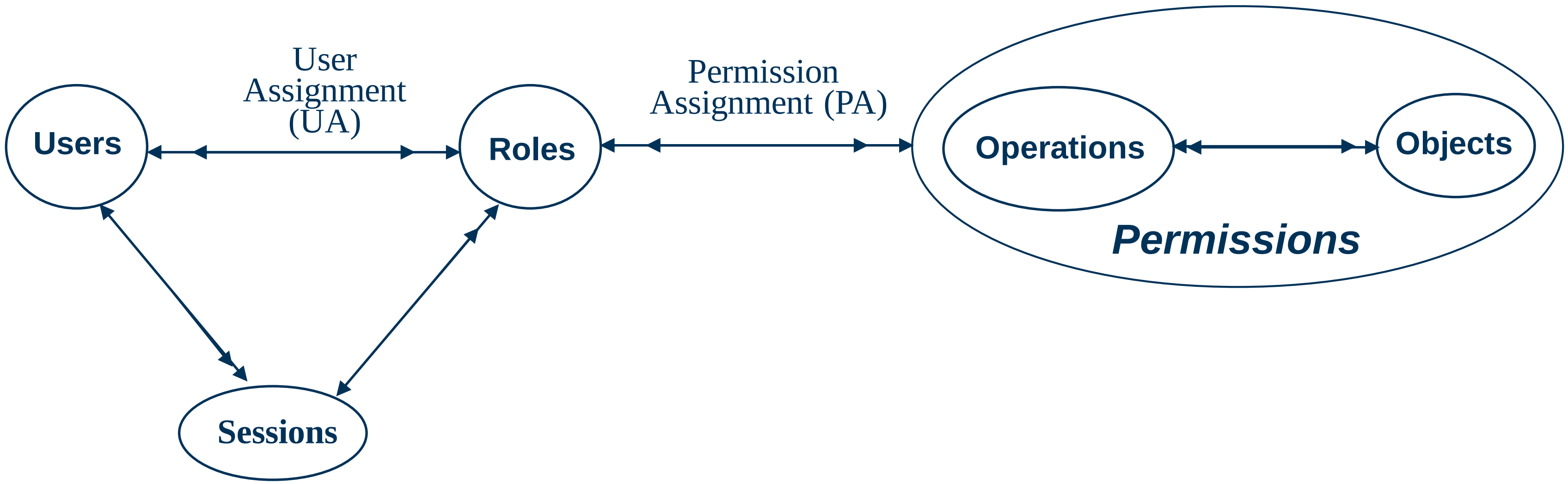
COMPSCI 702
Security for Smart-Devices

Muhammad **Rizwan** Asghar

March 10, 2021

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

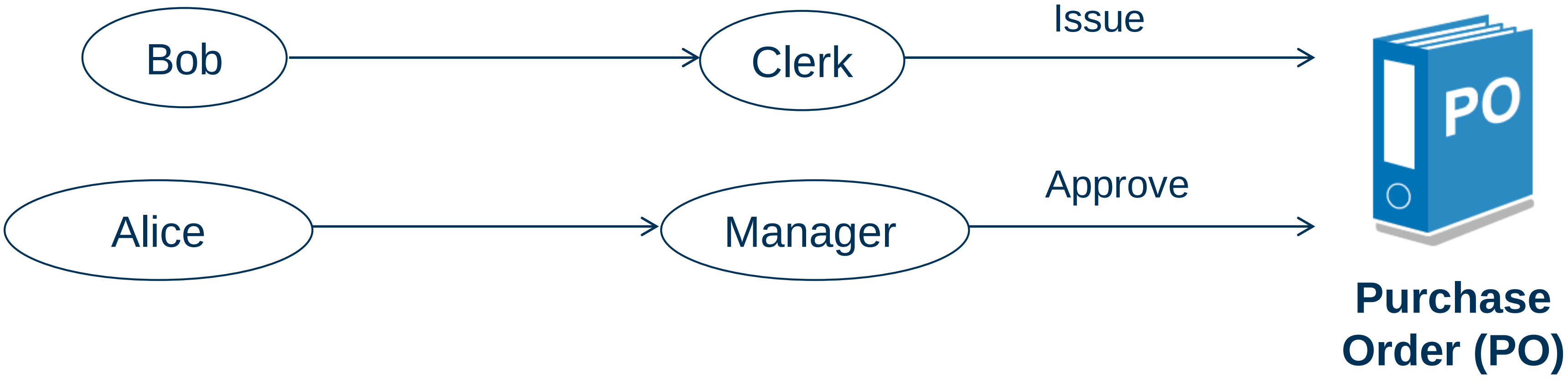
CORE RBAC



- Permissions represent what operations could be performed on objects
- Roles are assigned permissions: Permission Assignment (PA)
- Users are assigned roles: User Assignment (UA)
- Session is a mapping between a user and an activated subset of assigned roles

Revised image, originally from: Secure Systems Research Group at the Florida Atlantic University

RBAC EXAMPLE



Bob

Clerk

Issue

Alice

Manager

Approve

PO

Purchase Order (PO)

Bob, Clerk
Alice, Manager

Session

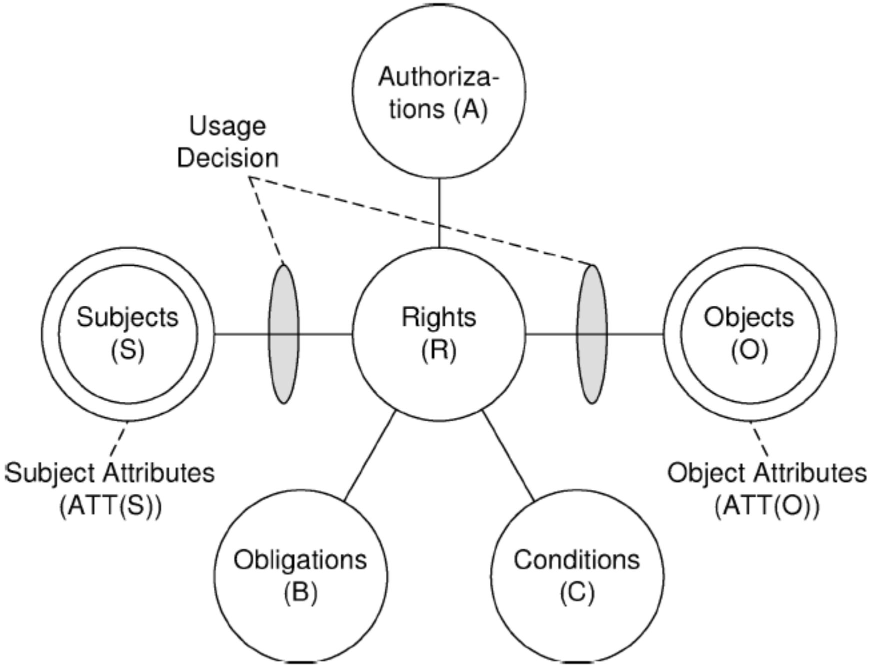
CONTROLLING USAGE OF RESOURCES

- DAC, MAC, and RBAC are concerned with checking access rights of entities
- Once the access is granted, no more control could be enforced
- Consider the following examples
  - Read a file only 5 times
  - Write data into a dir only up to 1 GB
  - Connect to the Internet only if there is enough balance
  - Withdraw from ATM only if there is enough credit in account

USAGE CONTROL (UCON)

- UCON not only regulates access to an object, but also focuses on controlling usage
- Addresses Digital Right Management (DRM) concerns
- DAC, MAC, and RBAC can also be expressed by UCON

UCON MODEL



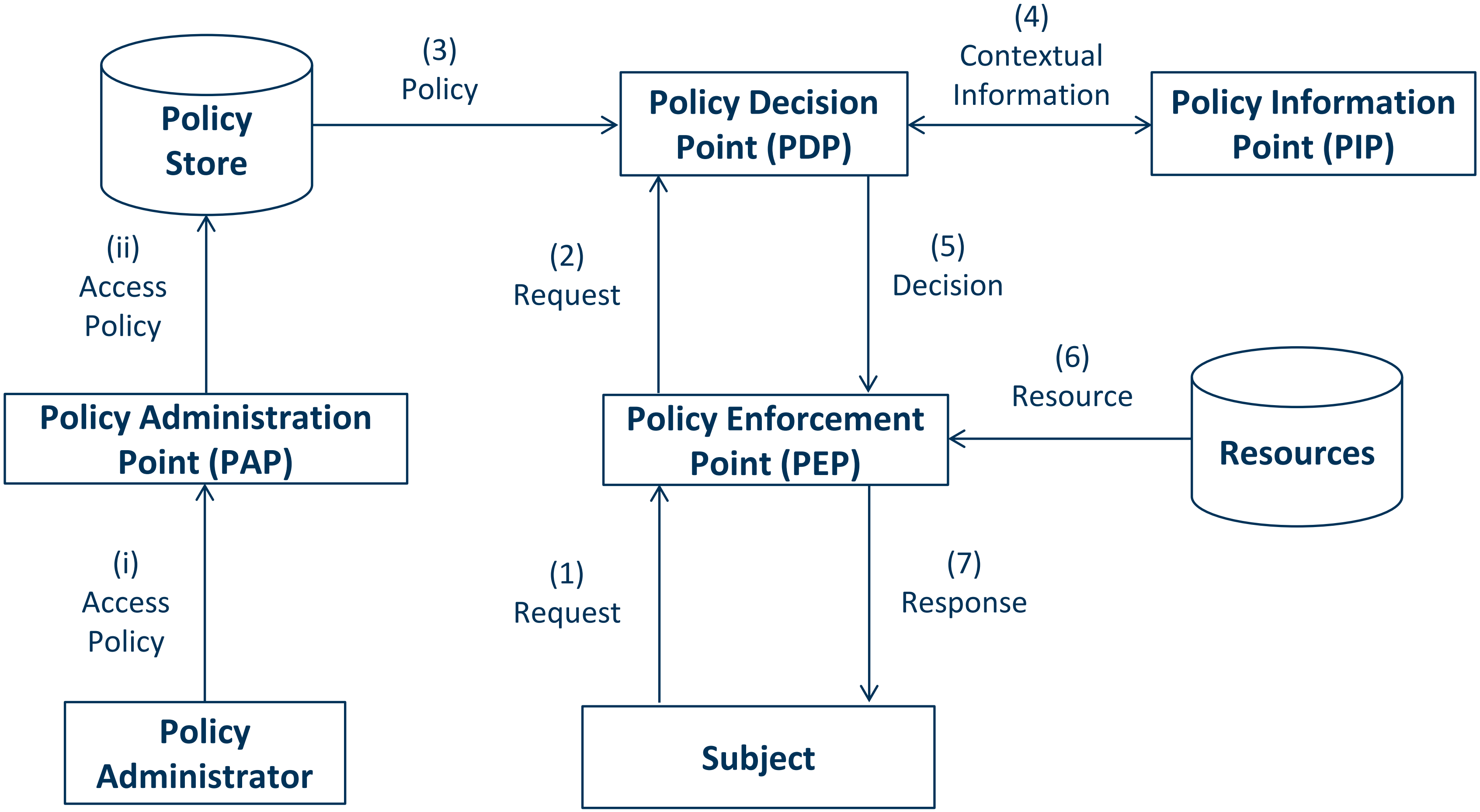
Source: [Park TISSEC04]

- Subjects
  - Entities that perform actions
- Objects
  - Entities that are accessed by subjects
- Rights
  - A set of actions
- Authorisation
  - Functional predicates that have to be evaluated for usage decision
- Obligations
  - Functional predicates that verify mandatory requirements that must have been performed by the subject
- Conditions
  - Environmental or system based decision factors (e.g., time and status)

POLICY-BASED ACCESS CONTROL (PBAC)

- In PBAC, an authorisation policy governs access rights of subjects over objects
- Policies are specified independently of entities
- Provide at a glance a coherent view of access control in a system
- Give a neat separation between access control logic and enforcement mechanism
- XACML is a typical PBAC approach
- E.g., *a GP can access medical records in office hours from her clinic*

PBAC MODEL



IETF RFC 2753

PBAC ENTITIES

- Policy Administrator
  - Administrates access policies
- PAP
  - An interface for policy administration
- Policy Store
  - A repository to store policies
- Subject
  - An entity that makes access requests
- Resources
  - Target objects requested by subjects
- PEP
  - Enforces access policies and grants access to resources
- PDP
  - Evaluates access policies to make a decision
- PIP
  - Provides contextual information

RESOURCES

- **Chapters 5 and 6 of**
  Information Security: Principles and Practice
  Mark Stamp
  Wiley 2011

- Sandhu, Ravi S., Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. "Role-Based Access Control Models." Computer 2 (1996): 38-47

- Park, Jaehong, and Ravi Sandhu. "The UCON ABC usage control model." ACM Transactions on Information and System Security (TISSEC) 7, no. 1 (2004): 128-174

- R. Yavatkar, D. Pendarakis, R. Guerin, A Framework for Policy-based Admission Control, RFC 2753

ACKNOWLEDGEMENT

- Some slides on DAC and MAC are based on the lecture delivered by Giovanni Russello, thanks to him!

Questions?

Thanks for your attention!