Access Control and Operating System Security

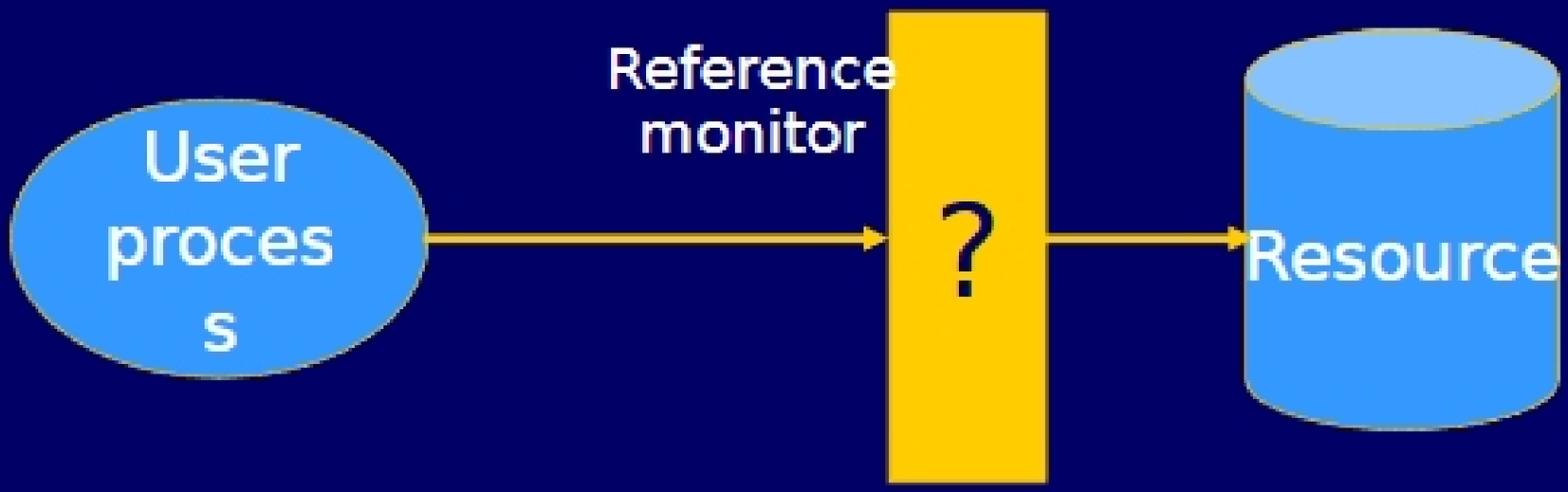
John Mitchell

Outline

- Access Control
  - Matrix, ACL, Capabilities
  - Multi-level security (MLS)
- OS Policies
  - Multics
    - Ring structure
  - Unix
    - File system, Setuid
  - Windows
    - File system, Tokens, EFS
  - SE Linux
    - Role-based
    - Domain type enforcement
- Secure OS
  - Methods for resisting stronger attacks
- Assurance
  - Orange Book, TCSEC
  - Common Criteria
  - Windows 2000 certification
- Some Limitations
  - Information flow
  - Covert channels

Access control

- Common Assumption
  - System knows who the user is
    - User has entered a name and password, or other info
  - Access requests pass through gatekeeper
    - Global property; OS must be designed so that this is true



Decide whether user can apply operation to resource