Access Control and Operating System Security

John Mitchell

Outline

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

Access control

- Assumptions
  - System knows who the user is
    - Authentication via name and password, other credential
  - Access requests pass through gatekeeper
    - System must not allow monitor to be bypassed