SC3010
Computer Security

Lecture 5: Operating System Security (I)

Security Challenges in Modern OS

From single-user to multi-user

- DOS is truly single user
- MacOS, Linux, NT-based Windows are multi-user
- Cloud computing allows multiple users all over the world to run on the same system, and they do not know each other.
- Not all users are trusted!

From trusted apps to untrusted apps

- Simple real-time systems: only run one specific app from trusted sources
- Modern PCs and smartphones: run apps from third-party developers
- Not all apps are trusted!

From standalone systems to networked systems

- Isolated computer systems only need to protect against physical threats.
- Once connected to networks, the system faces external unknown threats.
- Not all network components are trusted!

Outline

- **Security Protection Stages in OS**
  - Authentication
  - Authorization with Access Control
  - Logging, Monitoring & Auditing

- **Privilege Management in OS**

Outline

- **Security Protection Stages in OS**
  - Authentication
  - Authorization with Access Control
  - Logging, Monitoring & Auditing

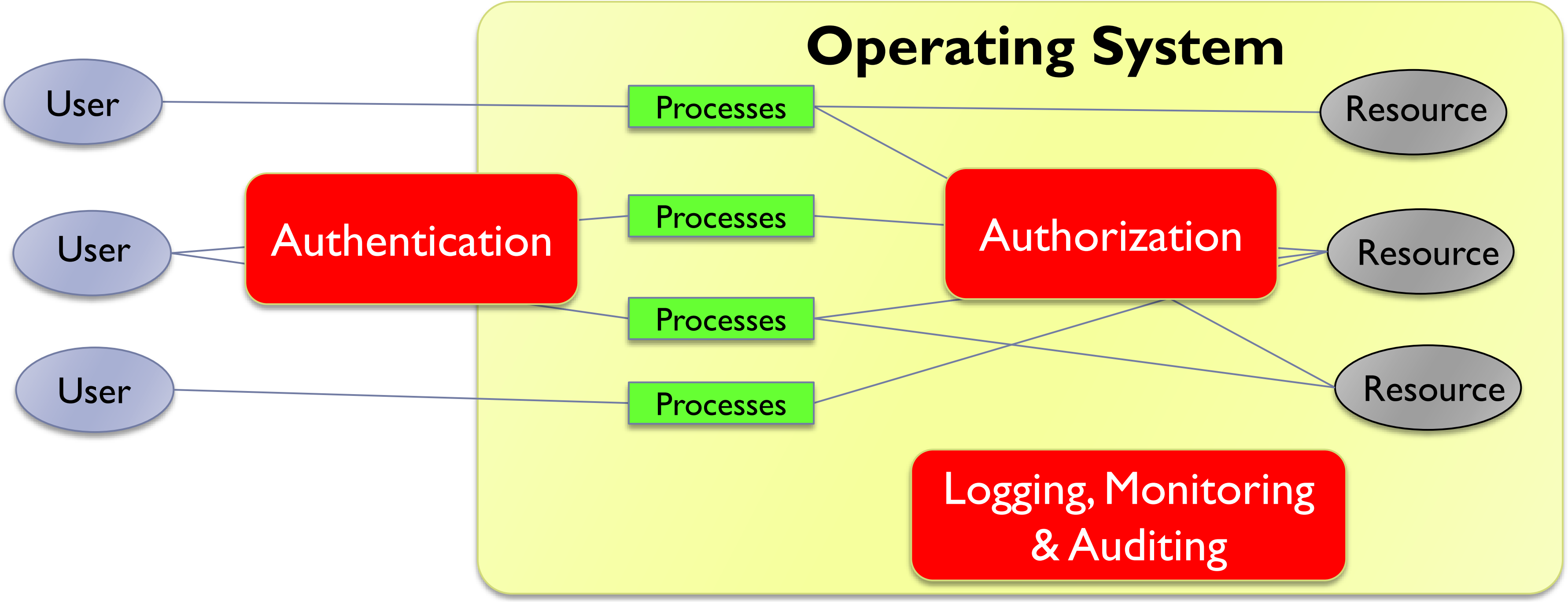
- **Privilege Management in OS**

Security Protection from OS

OS is responsible for protecting the apps and resources inside it.

- OS controls what users/processes can do
- OS prevents what users/processes cannot do

Protection Stages


Operating System
User
User
User
Authentication
Processes
Processes
Processes
Processes
Authorization
Resource
Resource
Resource
Logging, Monitoring & Auditing