

# IS 2150 / TEL 2810

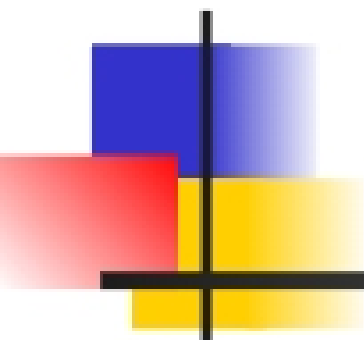
## Introduction to Security



James Joshi  
Assistant Professor, SIS

Lecture 2  
September 6, 2007

Secure Design Principles  
OS Security Overview



---

# Design Principles



# Design Principles for Security

---

- Principles
  - Least Privilege
  - Fail-Safe Defaults
  - Economy of Mechanism
  - Complete Mediation
  - Open Design
  - Separation of Privilege
  - Least Common Mechanism
  - Psychological Acceptability
- Based on the idea of *simplicity* and *restriction*