Design Principles and Trusted Operating Systems

CSCI283/172 Fall 2008
GWU

Draws extensively from Memon's notes, Brooklyn Poly
And Pfleeger text, Chapter 5

Need

- Policy: description of requirements
- Model: policy representation: check if policy can be enforced
- Design: implementation of policy
- Trust: based on features and assurance

Design Principles for Secure Systems

- Two basic themes:
  - Simplicity – KISS
    - Makes design and interactions easy
    - Easy to prove its safety
  - Restriction
    - Minimize the power of entities
    - Compartmentalization
- Common Sense!