• Full disclosure depends on attentives.
• Different levels of trust.
  ◦ Missiles Belongs to Trusted Computer Bases (TCB).
  ◦ Youtube does not belong to TCB.

Isolating untrusted component <- Topic

Trust is transitive

COST:
• Write code yourself
• Check code by multiple people
• Cross-check / replication
• Trusted authority for software

Core Secure System Design Principles
• Keep it simple (small TCB)
  "Economy of Mechanism"
• Failsafe defaults
  ◦ Default DENY – fails loudly
  ◦ Default ALLOW – fails silently
• Least Privilege
• Complete mediation
  ◦ Minimize access paths
• Separation of Privilege
Example:

- Least Shared Mechanism
  - Least Shared State
- Psychological Acceptability

TRAJECTORY OF COMPUTER SECURITY RESEARCH

Finer-grained and move-dynamic Controlled Sharing