- Full disclosure depends on alternatives

- Different Levels of trust
  - Missile System = TCB
  - Youtube != TCB

You trust login which means you trust the compiler, OS, OS source, login source, program loader, Intel, and China. We have to trust everything associated with login. **[Trust is transitive]**

We can cut trust edges by:

- --write code yourself.
- cost --> -check code by multiple people.
- --> -cross-check/replication

- Trusted authority for software
- - Full disclosure depends on alternatives.

**Core Secure System Design Principles**

- Keep it simple (small TCB)
  
  “Economy of mechanism”

- Failsafe Default (e.x. Default DENY – fails loudly, Default ALLOW – fails silently)

- Least Privilege (e.x. Amazon employees have more privileges to the database than the customer)

- Complete Mediation
  
  - Minimize access paths (fewer entrances)

- Separation of privilege (e.x. Two different people need to perform an action [turning two keys])

- Least Shared Mechanism
  
  - Last shared state (You can use the same type of database, but not use the same database for holiday recipes and government secrets.)

- Psychological Acceptability (e.x. Workers finding loophole to bypass a company’s computer system.)
Trajectory of Computer Security Research --------------→ Finer-grained and More-dynamic Controlled Sharing.