Paper Critique Discussion

- Different levels of trust: YouTube \( \not\in \) TCB; Missiles \( \in \) TCB
- Sometimes trust is transitive. E.g. Login Service

Ways of Ensuring Trust:

- Write code yourself
- Check code by multiple people
- Cross check (replication)
- Trusted authority for software
- Trust is bad
- Simplified design

Core Secure System Design Principles

1. Economy of Mechanism
2. Failsafe Defaults
3. Least Privilege
4. Complete Mediation
5. Separation of Privilege
6. Least Shared Mechanism
7. Psychological Acceptability

1. Economy of Mechanism
   - Keep it as simple as possible
   - Small and simple enough to be verified and implemented. E.g. Security kernel
   - Small TCB
2. **Failsafe Defaults**
   - Default in the system could be ‘default deny’ (fails loudly) or ‘default allow’ (fails silently)
   - For security, the default should be lack of access.
   - System would be as secure as before, even if the action fails.

3. **Least Privilege**
   - Only the rights necessary to complete the task should be granted
   - Default should be lack of access
   - Temporary access should be rescinded immediately after use
   - E.g. A Database system which is accessed from 2 web servers. One is the Customer webserver and the other the employee web server. Clearly, the customer web server should be allocated lesser privileges than the employee web server.

4. **Complete Mediation**
   - Secure all doors
   - Every access to every object must be checked
   - Minimize access paths

5. **Separation of Privilege**
   - Access to objects should be dependent on more than one condition being satisfied
   - Require two different people to sign (Separation of responsibilities)
   - Enable double checks
   - E.g. Mail server

   *Wrong Design*

   - Mail Server has sufficient privileges to send bug everywhere.
   - All functionalities in the same box.
Correct Design

![Diagram of network flow](image)

- Clear separation of privileges.
- Smaller TCB
- TCB doesn't have sufficient privileges to spread a bug

6. **LEAST SHARED MECHANISM**
   - Keep least shared state
   - Minimize the amount of mechanism common to more than one user and depended by all other users.
     - Keep separate account systems separate
   - Every shared mechanism is a potential information path

7. **PSYCHOLOGICAL ACCEPTABILITY**
   - The interface must be easy to use, so that users routinely apply the mechanisms correctly, otherwise they tend to be bypassed
   - Security mechanism should not add to the difficulty of accessing the resource
   - E.g. Psychological access causing failure of complete mediation as user tries to access firewall restricted area.

**Company Network**

![Diagram of company network](image)
TRAJECTORY OF COMPUTER SECURITY RESEARCH

- Isolation of mutually distrusting components
- Research towards achieving finer grained and more dynamic controlled sharing
- E.g. Security of mashups like Google Maps which is one the most mashed up web service