**Discussion on Locks paper**

- Full disclosure of locking system depends on the alternatives one have.
- Operating System bugs were forced to fix them since all and bad groups know about the bugs.

**Discussion on Untrusting Trust paper**

- There are different levels of trust.
  - a. Missile and military information belongs to Trusted Computing Base
  - b. Youtube information does not belong to Trusted Computing Base
- **Digital Rights Management**: DRM is an access control mechanism that limits the usage of digital contents and devices. This technology is like an agreement between people and industries to stop piracy.
- There is no end for trusting software. For example, in a simple login program, the login is dependent on various factors like login source, program loader, operating system in which the program is running, which is interdependent on operating system source code and factors like compiler and the version of the compiler. So there is no point in not trusting any one of the above factors.
- So the most cost effective trusted computing base would be:
  - c. Trust is transitive
  - d. Write code yourself
  - e. Check your code by multiple people
  - f. Cross checking/ replication
  - g. There should be a trusted authority which may authorize the trust factor of a code or program
  - h. Compile the code with different compilers and compare the output, errors and behaviour of the code.

**Core Secure System Design Principles**

- Keep in mind every step when you design secure system.
- Keep it simple (small TCB). This can also be called as "Economy of Mechanism".
- **Fail Safe defaults.**
  
  Eg: Anyone can overwrite C:/windows folder in windows operating system. In general Default DENY is more secure than Default ALLOW when user requests for something admin never mentioned. Default DENY fails more loudly where as Default ALLOW fails silently.

- **Least Privilege.**
  
  Eg: A database system is accessed by both Customer Web Server and Employee Webserver. In this case Customer Webserver is given least privilege than Employee Webserver because modifications to the database can not be made by customers.

- **Complete Mediation**: We should minimize access paths. One should look into complete access doors.

- **Seperation of privilege**: This means that to access a secure database or something, the authorization is given to more than 2 people. All the authorized people should be present in order to unlock the restricted area. The purpose of this is to enable double checks. Eg: Using two compilers to complie a specific piece of code.

  **Example: Mail Server**
  
  Consider a Mail Server which recieves a mail, forwards a mail and delivers or drops a mail. If all the privileges are given to one single mail server and if a worm is recieved by the mail server, it can spoil the entire system and forward, deliver all the spam mails to the recipients. So the alternative is to seperate the privileges to recieve and send functionalities.

  There should be seperate servers for recieve program and forward program where in once a mail is recieved it is queued to a validator which stands in between the recieve and forward servers. This validator has the only privilege to listen and queue the mail. This validator validates the mail checking for any worms or spams and then queues it to the forward mail server which internally does the required operation. If the validator finds a worm in the incoming message, the forward mail server just dequeues the mail. This looks like a trusted mail server. In this the recieve, validate and send previleges are seperated to different components. So the Trusted Computing Base focuses only on validator and is small.

- **Least Shared Mechanism:**
  
  This is like using different istances of same database for different usage. For example in Amazon a seperate instance of the database is used as Password Database, a seperate instance for User reviews and another for Products.

- **Psychological Acceptability**