Computer System Security
Lecture 1 notes.

1) What is computer Security?
   • Something that cannot be bypassed.
   • Complete mediation.
   • Not vulnerable to threats. Threats could be external or internal threats.
   • Trust boundaries i.e Trusted Computer Base (TCB). For example trusted computer base
could be a small chip as compared to computer that has many soft wares running on it.
   As larger the interactive points to the external world lesser is the trust.

2) Security Goals?

   **AVAILABILITY:** It means that people should access the services that are being available to them
   lets say they should be able to access the amazon webserver.
   Availability can be in danger by the following attacks.
   • Denial of Service attack:
     Dos attack can be performed by the following:
     1) By using the bandwidth of the network exhaustively so that other users don’t find
        enough bandwidth.
     2) By man in middle attack.
     3) TCP-SYN attack: for example each webserver has a limited amount of spaces for users
        before dedicated connection could be made. And dedicated connection is made by the
        following steps by first sending the TCP request. Then server sends SYN packet and then
        user computer sends ACK back to the server. If on completing the first two steps if user
        doesn’t send the ACK packet then space could be reserved on the server for this user as
        server is expecting the ACK packet back from user. So in this way user can make lot of
        incomplete connection which can lead to the usage of the of all no of connection a
        webserver can make. Hence leading to the unavailability of the service for other user.
   • Heavily using the OS resources of the system.
   • Crashing the system may be by ping of death attacks.
   • Account Locking: It can be done by using the excessive amount of the following.
     • CPU time
     • RAM
     • DISK

   **SECRECY:** Secrecy means that attacker should not know users
   • Password
• Credit card nos
• Trade secrets
• Business cards
• Source code
• SSN
• Contact information
• Anonymity: Hide who is talking to whom

**INTEGRITY:** It means that if sender sends some data to receiver on the network. And when data is received by the receiver then it should be same as it is send by the sender. Attacker should not modify the data on transit.
Data should only be modified in authorized way.
Only authorized person should modify the database contents
Only the required persons should modify the source code.

**EFFICIENCY:** Efficiency could be achieved by patching. Patching means fixing OS vulnerabilities and making system more efficient.


**SECURITY VS RELIABILITY?**
Security is the study of computing in the presence of attackers.
Attackers do not follow a known probability distribution.

**Threat Models?**
Threat models define the capabilities, goals and limitations of the attackers.
The limitations of the attacker are as follows:
1) Computational limitation: Attackers must have good computers that can do calculations very fast.
2) Bandwidth: Attackers must have good resources like bandwidth, connectivity etc.
3) Time: Attacker should complete the attack before session expires.
4) Access: It is also one of the limitations that attacker face. There could be two types of access.
   - Remote access: Which means attacker has an account on the server.
   - Local access: Which means that attacker has an account on the server which he want to attack.
5) Knowledge of the defenses: Attacker should the knowledge of everything except the explicity denoted secrets like passwords, encryption keys, random no’s.
Attacker should know have the knowledge of the
   - Encryption system.
   - Public keys info.
Logging system.
Partial knowledge of the data.
Location of the trap doors
Network layout.
Browser
Source code.