CSS Unit 2 Short Notes

Security Policies : It is a Statement that partitions the Computer States into Secure and Unsecured States , A Computer is said to be secure as long as it remains in the secure state and cannot enter an insecure state , a security breach may occur otherwise

Policy Model : A Model that represents a particular policy or a class of policies

Types Of Security Policies :

- Military Security Policy : Primarily focuses on providing confidentiality to sensitive information , Organizations using this policy should be able to overcome compromises in integrity and availability of the data

- Commercial Security Policy : Primarily focuses on maintaining the integrity of Data and preventing tampering of data , Organizations using this policy should be able to handle Loss of Confidentiality and limited availability

- Confidentiality Policy : This Policy Only Cares about Confidentiality , this may look similar to Military policy but , Military policy might be having some measures for integrity but Confidentiality Policy definitely Won't

- Integrity Policy : This Policy Only Cares about Integrity , may look like commercial policy but commercial might care about others but this policy cares about nothing else... Just Integrity

Role Of Trust in Computer Security :

Trust is fundamental to computer security , every policy , mechanisms and procedures rest on assumptions , so if one goes wrong , the security system will fail anyways regardless of how strong it is. So Trustworthiness of the System Security is Crucial

1) Security Measures Depend on Assumptions , you may install an anti virus with assumptions that it will be an authentic software etc...

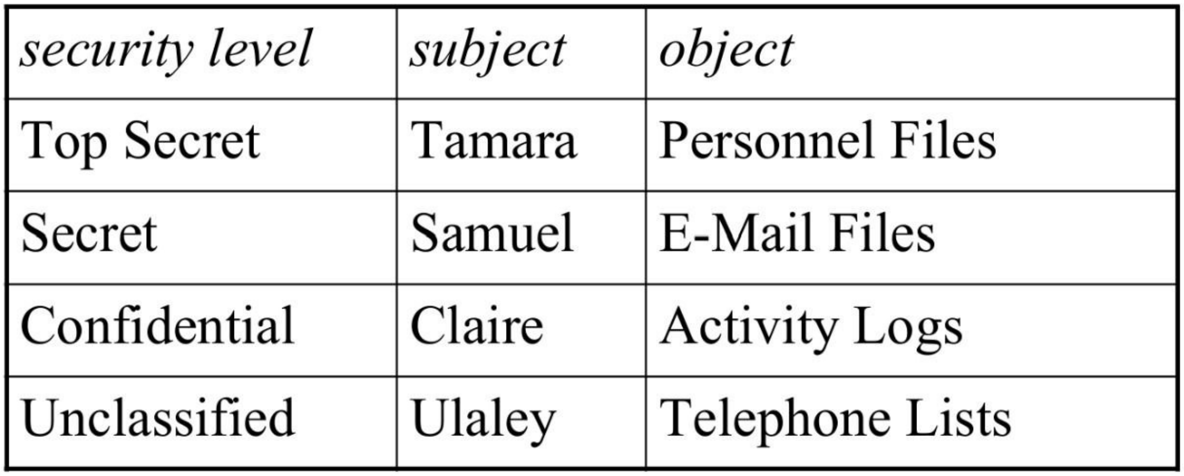
2) Wrong Assumptions can introduce new risks

3) Even Verified Programs depend on trust because maybe the verification process is corrupted who knows ?

4) A Single Broken Assumption will compromise the entire system

Confidentiality Policy : Policies that Focus on Maintaining the Confidentiality of the data , most widely used Model is Bell Lapadula Model

Bell Lapadula Model : It is a Famous (Mandatory Access Control) MAC model focused on Data Confidentiality , It is commonly used in Military and Government



security level	*subject*	*object*
Top Secret	Tamara	Personnel Files
Secret	Samuel	E-Mail Files
Confidential	Claire	Activity Logs
Unclassified	Ulaley	Telephone Lists

Key Rules of Bell Lapadula :

1) Simply Security Property : A Subject of A Certain Security Level can only read information from the Lower Security Levels to prevent Unauthorized access of Sensitive info , this Property is aka (NO READ UP!!! Rule)

2) Star (*) Security Property : A Subject of a Certain Security Level can only write information to the Higher Security Levels to prevent leakage of sensitive information to lower levels , aka (NO WRITE DOWN !!! Rule)