INTRO TO COMP-SEC

SECURITY PROPERTIES

1) Confidentiality

→ is the avoidance of the unauthorized disclosure of information

→ Tools to protect sensitive info use the ff. concepts:

- Encryption
- Access control
- Authentication
- Authorization
- Physical Security

2) Integrity

→ is about making sure tht info. has not been corrupted, changed or added to by human activity either during transit / in storage

- Backups
- Checksums
- Data correcting codes

3) Availability

→ is about making sure tht info. is accessible and modifiable in a timely fashion by those authorized to do so.

4) Assurance

→ refers to how trust is provided and managed in comp. systems

5) Authenticity

→ is about being certain tht. info received/accessed by us is from the entity we believe it to be from

6) Anonymity

→ is the property tht certain records / transactions not to be attributable to any individual

TRUST

→ Generally, we trust when we have:

1) Assurance

2) Reliability / Resilience

- The sys. shld operate intact in the face of natural disaster & human launched attacks

3) Accountability

- is about having the means to verify tht the sys. is operating as designed
- Log files, etc.

COMMON DEFENCE METHODS

1) Prevent

2) Deter — make it look like bad things will happen to you if you attack the sys.

3) Deflect — try to show another target to the adversary

4) Detect — If all the above fails, you can tell tht attack is happening

5) Recover — An attack has happened, how do you know you're now back in good state?