Main Objectives: Computer Security

There are 7 key concepts in the field of computer security:

1. Authentication (identity -solved by eg 2FA) crypto
2. Authorization (permission -solved by Access control list)
3. Confidentiality (secrecy contents -solved by encryption) crypto
4. Data/message integrity (unmodified-solved=msg auth code) crypto
5. Accountability (who is responsible -solved by log trail)
6. Availability (access –solved by adding redundancy)
7. Non-repudiation (undenialibility -solved by digital sig) crypto

AUTHENTICATION

- *Authentication* is the act of verifying someone’s identity, AND ESPECIALLY IMPT IN CYBERSPACE

AUTHORITY

- *Authorization* is the act of checking whether a user has permission to conduct some action.

CONFIDENTIALITY

- The goal of *confidentiality* is to keep the contents of a transient communication or data on temporary or persistent storage secret.

MESSAGE/DATA INTEGRITY

- When Alice and Bob exchange messages, they do not want a third party such as to be able to modify the contents of their messages.