First ppt.

CIA TRIAD

* **Confidentiality**: prevent/detect/deter improper **disclosure** of information
* **Integrity**: prevent/detect/deter improper modification of information
* **Availability**: prevent/detect/deter improper **denial of access** to services
* **And**
* Securing **computing resources**: prevent/detect/deter improper **use** of computing resources
  + Hardware
  + Software
  + Data
  + Network

Needed to achieve security

* **Organizational Goals :**Why to invest in security protection?
* **Policy :**hat to protect?
* **Mechanism**: How to protect?
* **Assurance**: How good is the protection?

TERMS

* **Threat**: potential occurrence that can have an undesired effect on the system
* **Vulnerability**: characteristics of the system that makes is possible for a threat to potentially occur
* **Attack**: action of malicious intruder that exploits vulnerabilities of the system to cause a threat to occur
* **Risk**: measure of the possibility of security breaches and severity of the damage

THREAT TYPES

* Errors of users
* Natural/man-made/machine disasters
* Dishonest insider
* Disgruntled insider
* Outsiders
* **Disclosure** threat – dissemination of unauthorized information
* **Integrity** threat – incorrect modification of information
* **Denial of service** threat – access to a system resource is blocked

Attack types

* **Interruption** – an asset is destroyed, unavailable or unusable (*availability*)
* **Interception** – unauthorized party gains access to an asset (*confidentiality*)
* **Modification** – unauthorized party tampers with asset (*integrity*)
* **Fabrication** – unauthorized party inserts counterfeit object into the system (*authenticity*)
* **Denial** – person denies taking an action (*authenticity*)
* **Passive attacks:**
  + Eavesdropping
  + Monitoring
* **Active attacks**:
  + **Masquerade** – one entity pretends to be a different entity
  + **Replay** – passive capture of information and its retransmission
  + **Modification** of messages – legitimate message is altered
  + **Denial of service** – prevents normal use of resources

Maliscous attacks

* Method: skills, knowledge, tools, information, etc.
* Opportunity: time and access
* Motive: reason to perform the action

Attackers

* **Amateurs**: regular users, who exploit the vulnerabilities of the computer system
  + Motivation: easy access to vulnerable resources
* **Crackers**: attempt to access computing facilities for which they do not have the authorization
  + Motivation: enjoy challenge, curiosity
* **Career criminals**: professionals who understand the computer system and its vulnerabilities
  + Motivation: personal gain (e.g., financial)

Defence methods

* **Prevent**: block attack
* **Deter**: make the attack harder
* **Deflect**: make other targets more attractive
* **Detect**: identify misuse
* **Tolerate**: function under attack
* **Recover**: restore to correct state

Ppt 2.

C. protocols

* Messages should be transmitted to destination
* Only the recipient should see it
* Only the recipient should get it
* Proof of the sender’s identity
* Message shouldn’t be corrupted in transit
* Message should be sent/received once only

TERMS

* **Plaintext** (**cleartext)**: a message in its original form
* **Ciphertext** (**cyphertext)**: an encrypted message
* **Encryption**: transformation of a message to hide its meaning
* **Cipher**: cryptographic algorithm. A mathematical function used for encryption (encryption algorithm) and decryption (decryption algorithm).
* **Decryption**: recovering meaning from ciphertext
* **Cryptography**: art and science of keeping messages secure
* **Cryptanalysis**: art and science of breaking ciphertext
* **Cryptology**: study of both cryptography and cryptanalysis

Obj.

* Confidentiality
* Integrity
* Availability
* Authenticity
* Non-repudiation
* **Confidentiality:** Hiding message/file content
  + Secret key, public key encryption
* Integrity: Detecting modification
  + Hash function
* Availability: Not much – hiding existence of data
  + Secret key, public key encryption
* Authenticity: Verify origin
  + Public key encryption
* Non-repudiation: Verify activity
  + Public key encryption