Introduction

Dr. B C Dhara
Department of Information Technology
Jadavpur University

Books

1. Cryptography Theory and Practice by Stinson
2. Handbook of Applied Cryptography by Menezes, Oorschot, Vanstone
3. Forouzan, Cryptography & Network Security, Tata McGraw-Hill

SECURITY GOALS

- We are living in information age
- Information is grate assets, it needs to be secured from attacks
  - To be secured, information needs to be
    - Hidden from unauthorized access (confidentiality)
    - Protected from unauthorized changed (integrity)
    - Available to an authorized person when needed (availability)

SECURITY GOALS (Contd…)

- Previously, information of an organization was stored in a physical file
  - Confidentiality was achieved by restricting the access to a few authorized and trusted people
  - Few authorized people are allowed to change the contents of the files
  - Availability was achieved by designating at least one person who would have access to the files at all times

SECURITY GOALS (Contd…)

- At the computer age, information become digital and stored in computer
- Files stored in computer also required confidentiality, integrity and availability
  - Implementation of these are different and challenging

SECURITY GOALS (Contd…)

- Computer networks created revolution in the use of information
  - Information is now distributed
  - People can send and retrieved information from a distance through computer network
    - Above three requirements have not changed
      - Now they have new dimension
      - Not only it has to be maintained the security when stored in computer, also have to be maintain the security when transmitted from computer to computer

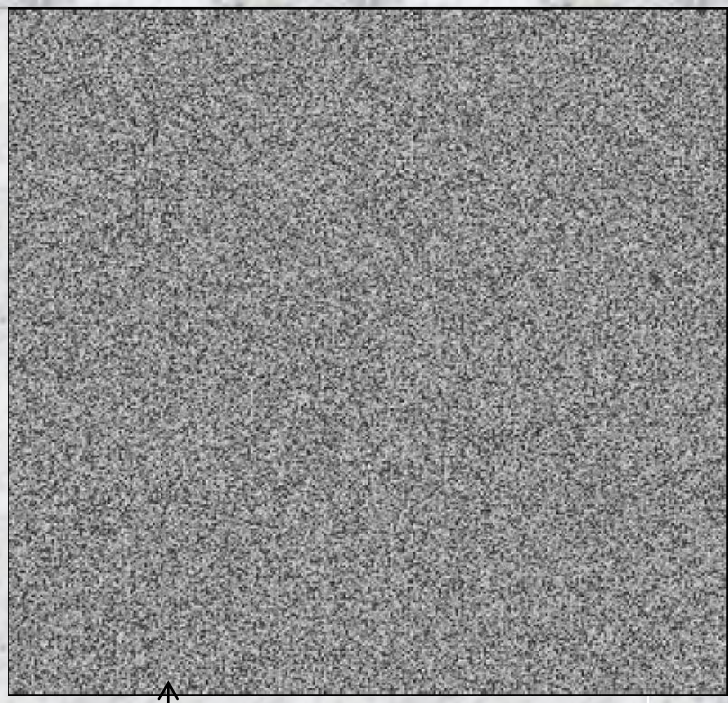
SECURITY GOALS (Contd…)

- We will study
  - three major goals of information security
  - Attacks on these goals
  - Define security services and how they are related to the three security goals
  - Security mechanisms to provide security services
  - Techniques,
    - Cryptography, Secret sharing, watermarking and steganography, to implement security mechanisms

Possible solutions

- Cryptography
  - Cryptography is about protecting the content of messages
  - Scramble message to make it meaningless
- Hiding
  - Steganography is about concealing the existence of messages
  - Hide the existence of communication
- Watermarking
  - Watermarking is about establishing identity of information to prevent unauthorized use by hiding a message about the media
- Secret sharing
  - Divide the secret into pieces, distributed to participants and authorized subset of participants can recomputed the secret

Example cryptography



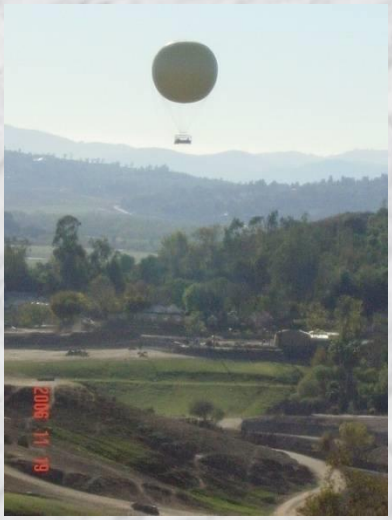
Key

Algorithm

Data hiding (Steganography)

Secret message

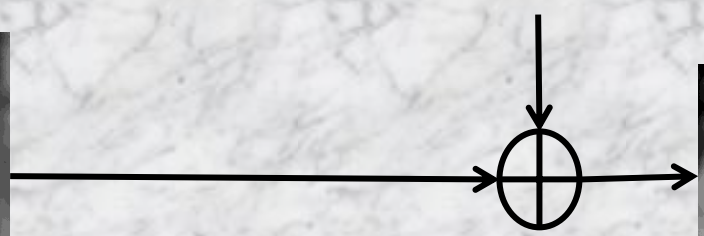
Cover Image



Stego Image

Watermarking

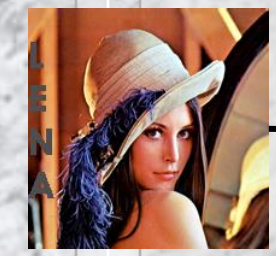
Watermark image



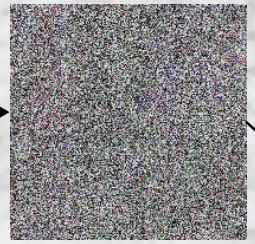
Original image

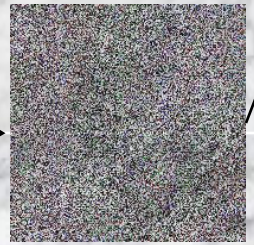
Watermarked image

Secret sharing



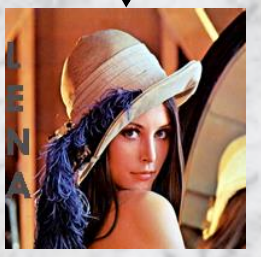
Sharing algorithm





Select any 3 shares out of 4

Reconstruction algorithm



SECURITY GOALS (Contd…)

Taxonomy of security goals

Confidentiality

- Confidentiality is probably the most common aspect of information security. We need to protect our confidential information
  - An organization needs to guard against those malicious actions that endanger the confidentiality of its information
    - In military, concealment of sensitive information is major concern
    - In industry, hiding information from competitors is crucial
    - We need to conceal information during transmission

Integrity

- Information needs to be changed constantly
- Integrity means that changes need to be done only by authorized entities and through authorized mechanisms
  - Integrity violation not necessary a malicious act
    - Due to power failure, at the time of updation, unwanted changes in some information

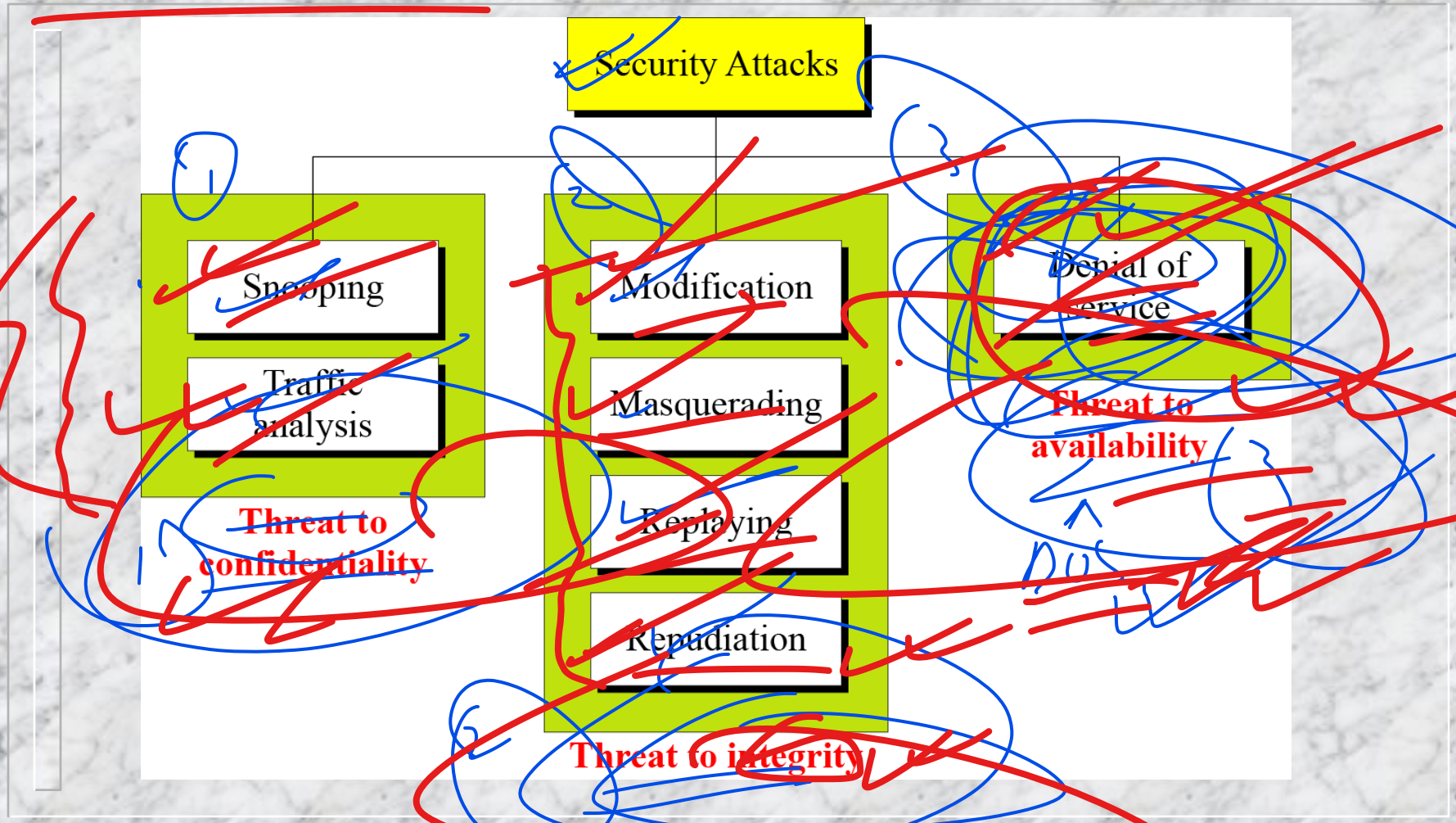
Availability

- The information created and stored by an organization needs to be available to authorized entities
  - Information is useless if it is not available
- Information needs to be constantly changed, which means it must be accessible to authorized entities

Attacks

- The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks
- Attacks divided into three groups related to the security goals:
  - Threatening Confidentiality
  - Threatening Integrity
  - Threatening Availability

Taxonomy of attacks with relation to security goals



Attacks Threatening Confidentiality

- ***Snooping*** refers to unauthorized access to or interception of data
  - A file transferred through Internet and a third party intercepts the transmission and use for own benefits
- ***Traffic analysis*** refers to obtaining some other type of information by monitoring online traffic
  - Third party can find e-mail of the sender or receiver

Attacks Threatening Integrity

- Modification means that the attacker intercepts the message and changes it
  - For own benefits, e.g., request from a customer to bank
- Masquerading or spoofing happens when the attacker impersonates somebody else
  - Attacker steal bank card and Pin of a customer and pretend himself as that customer, or
  - a user tries to contact a bank, but another site pretends that it is the bank and obtains some information of the customer

Replay attack

- The attacker obtains a copy of a message sent by a user and later tries to replay it
  - A person send a request to bank to ask for payment to the attacker, who has done a job for her
    - Attacker send the same message again to receive another payment

Repudiation attack

- Sender of the message might later deny that she has sent the message;
  - A customer asked his bank to send money to a third party but later deny that she has made such request
- Receiver of the message might later deny that he has received the message
  - A customer buys a product from a company and pays for it electronically, but later the company has denied the received of the payment and ask for payment again

Attacks Threatening Availability

- Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.
  - An attacker might send so many bogus requests to a server that server crashes due to heavy load
  - Attacker might intercept and delete server's response, client may believe that the server is not responding

Attacks (Contd…)

- Classification of attacks based on their effects on the system
  - Passive attacks
  - Active attacks

Passive attacks

- Attacker's goal is to obtain information
  - No modification, no harm to system
  - System continues its normal operation
  - May harm the sender or the receiver

Active attacks

- May change the data or harm the system

Categorization of passive and active attacks

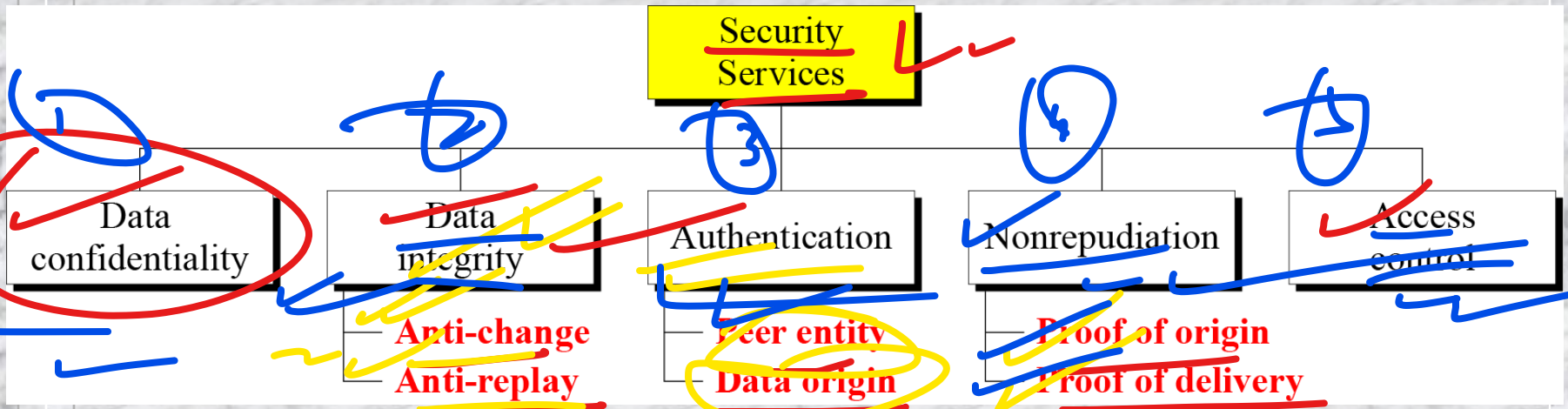
Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Security Services and Mechanisms

- ITU-T provides some security services and some mechanisms to implement those services.
  - Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service and a mechanism may be used in different services

Security Services

- ITU-T (X.800) has defined five services related to the security goals and attacks



Security services (Contd…)

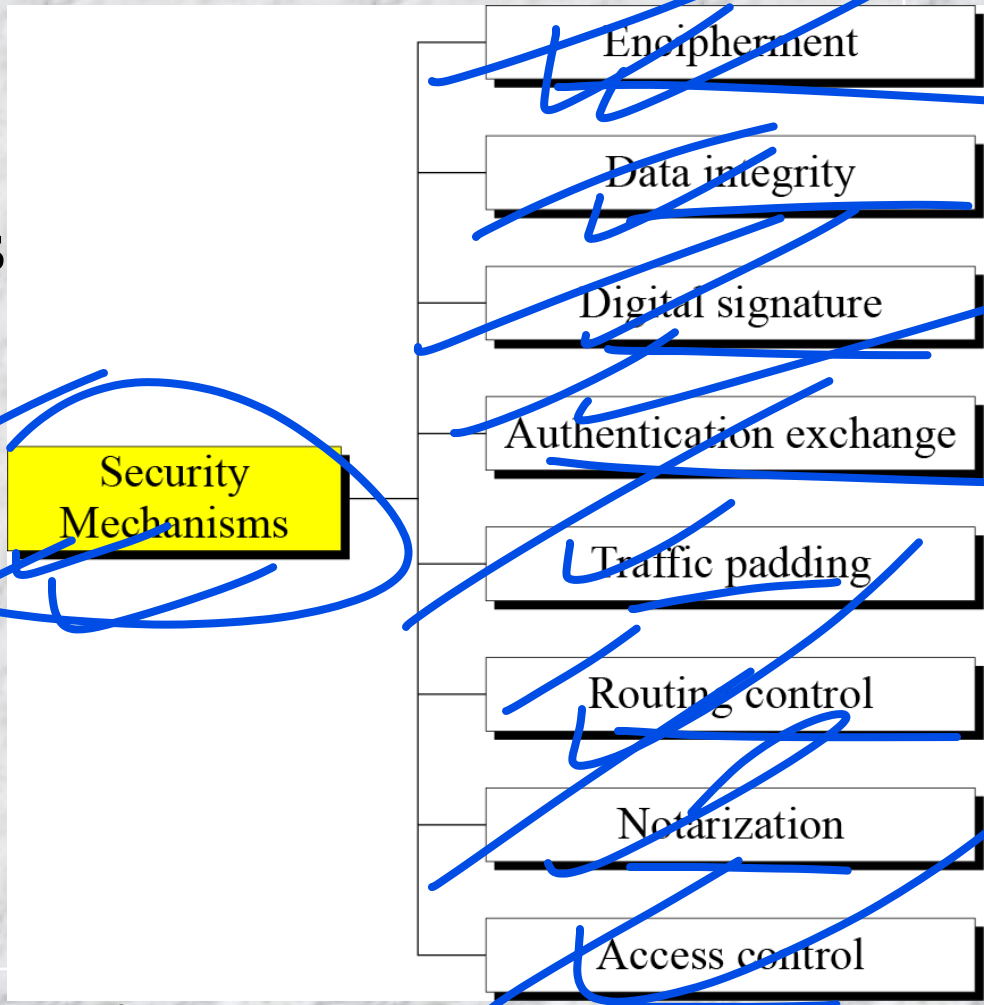
- Data confidentiality is designed to prevent snooping and traffic analysis attack
- Data integrity is designed to protect data from modification, insertion, deletion, and replaying by an adversary
- Authentication includes the authentication of the party at the other end of the line (in case of connection oriented communication) and authenticates the source of data (in connectionless communication)

Security services (Contd…)

- Nonrepudiation service protects any repudiation by either sender or receiver
  - With proof of origin, the receiver can later prove the identity of the sender if denied
  - With proof of delivery, the sender can later prove that data were delivered to the intended recipient
- Access control protects data against unauthorized access
  - Access may involve reading, writing, modifying, executing program, etc.

Security mechanisms

- ITU-T recommends some security mechanisms to provide the security services



Security mechanisms (contd…)

- Encipherment mechanism includes two techniques cryptography and steganography to provide confidentiality
- Data integrity mechanism appends check value (computed by certain process) to the data
  - Receiver received data and check value and recomputed new check value and compare with old one

Security mechanisms (contd…)

- Digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature
  - Using private key, public key pair
- Authentication exchange established the identity of the sender and receiver through exchanging some messages

Security mechanisms (contd…)

- Traffic padding inserts some bogus data into the data traffic to resists the adversary's attempt to use the traffic analysis
- Routing control changes different available routes between the sender and receiver continuously to prevent the eavesdropping on a particular route

Security mechanisms (contd…)

- Notarization means selecting a third party to control the communication between two parties
  - Prevent repudiation
- Access control establish that a user has access right to the data or resources owned by the system
  - Use of password and PIN

Relation between Services and Mechanisms

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

TECHNIQUES

- Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques
- Two techniques are prevalent today:
  cryptography and steganography.

Cryptography

- Cryptography, a word with Greek origins, means ***secret writing***
- Cryptography refer to the science and art of transforming messages to make them secure and immune to attacks
- Cryptography referred to encryption and decryption of messages using secret keys
  - Symmetric-key cryptography
  - Asymmetric-key cryptography
  - hashing

Steganography

- The word steganography, with origin in Greek, means ***covered writing***

Thank You