Overview
on
Modern Cryptography

Debdeep Mukhopadhyay

Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

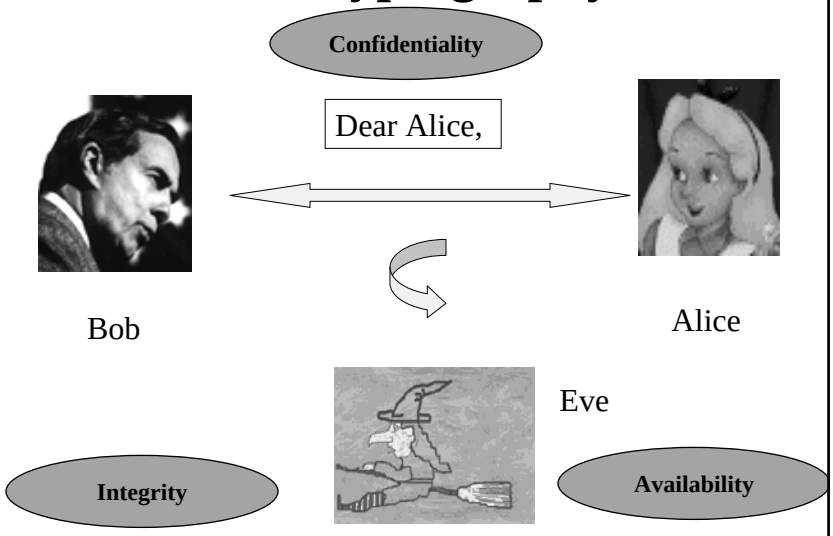
Objectives

- **Goals of Cryptography**
- **Security Services**
- **Security Mechanisms**
- **Relationship between the services and mechanisms**

The Three Goals

- **Confidentiality: hiding information from unauthorized access**
- **Integrity: preventing information from unauthorized modification**
- **Availability: should be easily available to authorized users**

Goals of Cryptography



Confidentiality

- **Information is exchanged over the un-trusted network.**
- **Information, while exchange, should remain secret.**
- **Confidentiality related to both the storage as well as transmission of information.**

Integrity

- **Information is always changing.**
- **But the change should be made by authorized users**
  - **modification: change made by unauthorized users.**
- **Need techniques to ensure the integrity of data:**
  - **preventing the modification**
  - **detect any modification made**

Availability

- **Confidentiality and Integrity should not hinder the availability of data.**
- **Data must be available to authorized users.**
- **Cryptographic mechanisms should have a small overhead.**

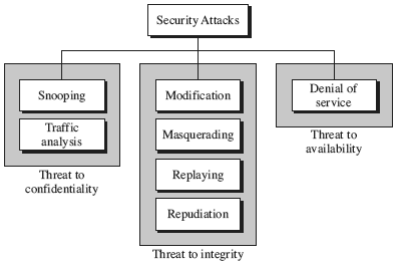
Mechanisms

- **Cryptographic Algorithms are used to achieve the above goal.**
- **They rely on a secret piece of information, called the key.**
- **The algorithms are published.**
- **Attackers objective is to obtain the key from the communication.**

Cryptographic Attacks

- **Cryptanalytic Attacks:**
  - **Applies mathematical techniques to obtain the key better than a brute force search (try all possibilities)**
- **All attacks are distinguishers:**
  - **all (good) ciphers transforms the plaintext distribution to "appear" as random.**
  - **the goal of an attack is to find properties in the cipher which does not exist in random distribution.**
  - **Attacker guesses a portion of the key and checks for the property.**
  - **Any attack better than a brute force search qualifies as an attack.**
  - **May not be practical but exposes design flaw.**

Non-cryptanalytic Attacks



- **Do not exploit the mathematical weakness of the cryptographic algorithms.**

Threat to Confidentiality

- **Snooping: Refers to unauthorized access or interception of information. Encryption is used to make information non-intelligible to the snooper.**
- **Traffic Analysis: Even an encrypted message can be analyzed to obtain some information, like say the identity of the sender and the recipient, the nature of information (like text or image files).**

Threat to Integrity

- **Modification: An attacker can modify the transmitted information, without needing to know the actual content.**

  It could delay or change the content to foil the objective of a transaction.
- **Masquerading: An attacker can modify the communication data to pretend (spoof) as a legal sender or receiver to obtain the information to which it does not have access.**

Threat to Integrity

- **Replaying: An attacker copies a message sent by a different user and replays later.**
- **Repudiation: Sender of a message may later deny that it has sent it. Example, a user may deny a third party payment request.**

  A receiver of a data may also refuse the receipt. Example, a merchant may refuse the receipt of a credit card payment. It is obvious, that cryptography should guarantee non-repudiation in these applications.

Threat to availability

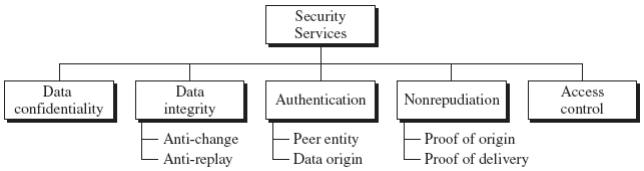
- **Denial of Service (DoS):**
  - **Slow down or totally disable the system.**
- **Example:**
  - **slow down the system with multiple requests.**
  - **delete the acknowledgements from the server**

Passive vs Active attacks

Attacks	Passive/Active	Goal Threatened
Snooping Traffic Analysis	**Passive**	**Confidentiality**
Modification, masquerading, replaying,repudiation	**Active**	**Integrity**
DoS	**Active**	**Availability**

Security Services

- **International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) provides some security mechanisms to achieve security services.**



Security Services

- **Confidentiality of part or full of message, prevent snooping and traffic analysis.**
- **Data Integrity: protect data from modification, insertion, deletion and replay.**
- **Authentication: ensures the sender or receiver of the information communicated.**
- **Non-repudiation: Protects by providing proofs against repudiation by either the sender or the receiver.**
- **Access Control: Provides protection against unauthorized use of data.**

Security Mechanisms

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

Security Mechanisms

- **Encipherment: Hiding information by encryption, steganography. It may be used for other services also along with other mechanisms, like for authentication, non-repudiation etc.**
- **Data Integrity: A small checksum (hash) value for a message is appended and sent. The receiver checks for the validity of the checksum.**

Security Mechanisms

- **Digital Signature: Sender can electronically sign an information, and a receiver can verify it.**
- **Authentication: Two parties can exchange information to prove to each other that they are communication, and not being masqueraded.**

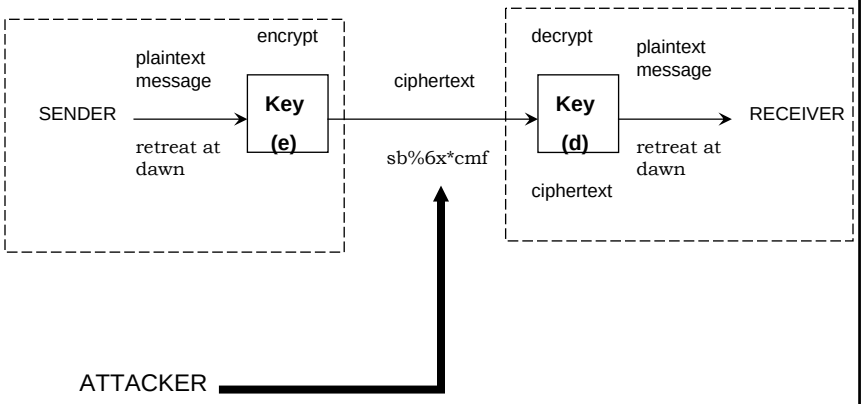
Security Mechanisms

- **Traffic Padding: Inserting bogus data to prevent traffic analysis.**
- **Routing Control: To select and change available channels of communication to make the attacker's job harder.**
- **Notarization: To have a trusted third party to control the communication.**
- **Access control: uses methods to prove that users have access to information, via passwords or PIN.**

Relationships between services and mechanisms

Services	Mechanisms
Confidentiality	Encryption, routing control
Integrity	Digital Signature, Encryption
Authentication	Encryption, Digital Signature
Non-repudiation	Digital Signature, Notarization
Access Control	Interactive Proofs, access control mechanisms and policies.

Techniques: Cryptographic Algorithms



Types of Cryptographic Algorithms

- **Symmetric Key Ciphers: The sender and the receiver share the same piece of key for their message exchange.**
- **Asymmetric Key Ciphers: The sender encrypts the message using a public key and the receiver decrypts using a secret (or private) key.**

Types of Cryptographic Algorithms

- **Hash Functions:**
  - **Produces a small check sum for a large message.**
  - **It is usually appended and sent with the message.**
  - **If the message is modified, then the receiver computes the hash value and checks for a match.**

Steganography

- **Word derived from Greek means covered writing.**
- **Historical facts and myths exist.**
- **A simple method used by Romans and Greeks, was to write on wood and then cover with wax.**

Modern Techniques

- **Cover of secret data can be text. Consider an English statement:**

This is an example of Steganography

Note the number of blanks between the words. Denote a single blank by 0, and two blanks by 1.

Thus we have the hidden message as: 01010

Modern Techniques

- **The cover can be image also.**
- **A colored digitized image is represented by 3 bytes.**
- **Each byte denotes Red, Blue, Green pixels.**
- **The technique for hiding a data in the image, uses the fact that a change in the LSB is not noticeable.**
- **Thus a message is secretly crafted in the LSBs of the digitized image and transmitted.**
- **There are several other more sophisticated techniques.**

Points to Ponder

- **Define the type of security attack:**
  - **A student steals the question paper.**
  - **I buy a book through credit card for Rs 2000, but find in my bank account that Rs 4000 has been paid..**
  - **One receives hundreds of emails from a colleague from an anonynous email account.**
- **Think of possible security mechanisms to prevent these attacks.**

References

- **B. A. Forouzan, *"Cryptography and Network Security",* TMH**

Next Days Topic

- **An Introduction to Number Theory**