

# Information Security and Cryptography (CS302)

## B.Tech. III (CSE) - Semester 6

Sankita Patel

Sardar Vallabhbhai National Institute of Technology

*[sjp@coed.svnit.ac.in](mailto:sjp@coed.svnit.ac.in)*

January 8, 2024

# Objectives & Outcomes

## Course Outcomes

After successful completion of this course, student will be able to

- 1) Understand the concepts related to Information Security and Cryptography
- 2) Apply the concept of security services and mechanisms from the application developers and network administrator's perspective.
- 3) Analyse the security schemes for their use in different application scenarios.
- 4) Evaluate and assess the computer and network systems for associated risks.
- 5) Design the security schemes depending on the organisation's requirements.

# Syllabus

- ▶ **INTRODUCTION** : Security Attacks, Services and Mechanisms, CIA Traid, Security Design Principles, Attack Surface and Attack Trees, Model for Network Security, Introduction to Number Theory, Shannon's Theory
- ▶ **SYMMETRIC KEY CIPHERS** : Substitution Techniques, Transposition Techniques, Digital Watermarking and Steganography, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Block Cipher Modes of Operation, Random Bit Generation and Stream Ciphers
- ▶ **ASYMMETRIC KEY CIPHERS** : Principles of Public-Key Cryptosystems, RSA, Diffie-Hellman Key Exchange, Elgamal Cryptosystem, Elliptic Curve Cryptography.
- ▶ **CRYPTOGRAPHIC HASH FUNCTIONS** : Hash Functions and Data Integrity, Security of Hash Functions-The Random Oracle Model, Iterated Hash Functions- Merkel Damgard Construction, Secure Hash Algorithm (SHA).

# Syllabus...

- ▶ **MESSAGE AUTHENTICATION** : Message authentication requirements, message authentication codes (MAC) based on hash functions-HMAC and block ciphers-DAA and CMAC, Authenticated Encryption-CCM and GCM
- ▶ **DIGITAL SIGNATURES** : Security requirements, RSA Digital Signatures, NIST Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), RSA-PSS Digital Signature Algorithm
- ▶ **IDENTIFICATION SCHEMES AND ENTITY AUTHENTICATION** : Challenge Response Protocols, Password Based Authentication, Zero Knowledge Schemes.

## Books

1. William Stallings, Cryptography and Network Security – Principles and Practice, 7th Edition, Pearson Education, 2013.
2. Forouzan and Mukhopadhyay, Cryptography and Network Security, 3rd Edition, McGraw Hill, 2015.
3. Menezes Bernard, Network Security and Cryptography, 1st Edition, Cengage Learning India, 2010.
4. D Douglas Stinson, Cryptography: Theory and Practice, 3rd Edition, CRC Press, 2006.
5. William Stallings, Network Security Essentials: Applications and Standards, 3rd Edition, Pearson Education, 2009.
6. Menezes, Oorschot and Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
7. Dhiren Patel, Information Security: Theory and Practice, PHI, 2008.

And reference reading material for some topics

# Grading

Theory: 50% Internal (30% Midterm Exam, 20% Continuous Evaluation) 50% Endterm Exam

Lab: 50% Internal 50% Endterm Exam

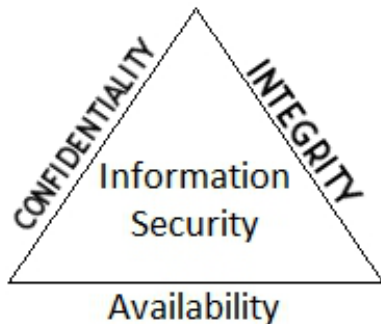
Tutorial: Internal grading only

# Definition of Computer Security

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources  
[NIST Computer Security Handbook, 95]

# Security Goals

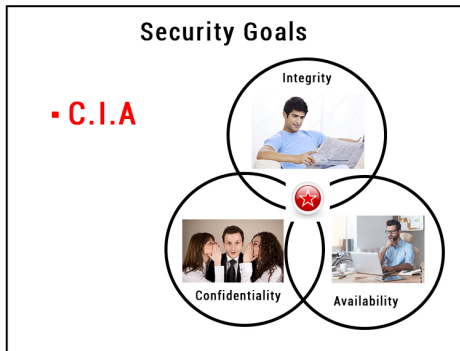
The CIA Triad





# Security Goals...

## The CIA Triad



# Security Goals...

- ▶ Confidentiality -
  - ▶ Data Confidentiality
  - ▶ Privacy
- ▶ Integrity
  - ▶ Data Integrity
  - ▶ System Integrity
- ▶ Availability
  - ▶ Assures that the system works promptly and service is not denied to authorized users
- ▶ Authenticity
- ▶ Accountability

# Example

- ▶ Levels of impact on an organization due to security breach
  - ▶ Low : Limited adverse effect on organizational operations, organizational assets and individuals
  - ▶ Moderate: Serious adverse effect.
  - ▶ High : Catastrophic adverse effect.
- ▶ Examples
  - ▶ Student Grade Information in University
  - ▶ Patient's allergy information in Hospital
  - ▶ Website that offers forum to registered users to discuss some specific topic
  - ▶ Anonymous online polls for news channels

# Security Attacks

The three goals of security i.e. confidentiality, integrity, and availability can be threatened by security attacks.

**Cryptanalytic Attacks** Combination of statistical and algebraic techniques aimed at ascertaining the secret key of a cipher. Ideally all cryptographic algorithms act upon the message distribution and convert it using the key to a ciphertext distribution which looks random.

The goal of an attacker is to find properties of the cipher which does not exist in a random function with an aim to mount an attacks faster than *the brute force attack*.

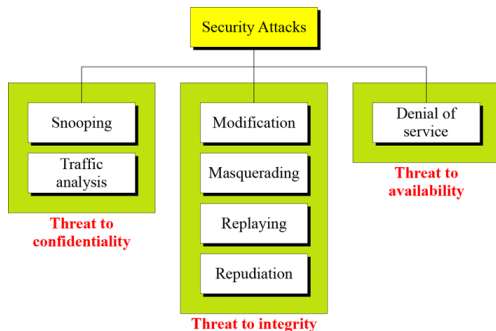
**Non-cryptanalytic Attacks**

Do not exploit the mathematical weakness of the cryptographic algorithm.

Much threat due to these attacks

# Security Attacks...

The three goals of security i.e. confidentiality, integrity, and availability can be threatened by security attacks.



# Security Attacks...

- ▶ Attacks threatening confidentiality
  - ▶ **Snooping** refers to unauthorized access to or interception of data.
  - ▶ **Traffic analysis** refers to obtaining some other type of information by monitoring online traffic.
- ▶ Attacks threatening Integrity
  - ▶ **Modification** means that the attacker intercepts the message and changes it.
  - ▶ **Masquerading** or spoofing happens when the attacker impersonates somebody else.
  - ▶ **Replaying** means the attacker obtains a copy of a message sent by a user and later tries to replay it.
  - ▶ **Repudiation** means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.
- ▶ Attacks threatening Availability
  - ▶ **Denial of service (DoS)** is a very common attack. It may slow down or totally interrupt the service of a system.

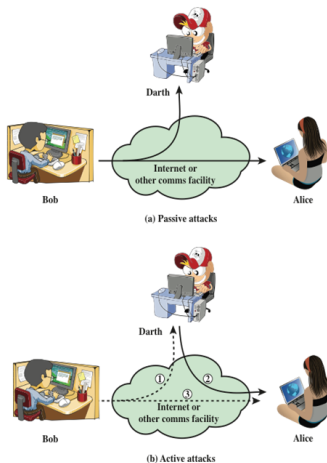
# Passive Vs Active Attacks

In **Passive Attack** attacker's goal is just to obtain information. The attack does not modify the data or harm the system. The system continues with its normal operation.

In **Active Attack** attacker may change data or harm the system.  
**Which one is easier to mount? Which one easier to detect?**

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

# Passive Vs Active Attacks...



**Figure:** Courtesy: Cryptography and Network Security by William Stallings



# Security Services

**Defined by X.800 as:** A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers

**Defined by RFC 4949 as:** A processing or communication service provided by a system to give a specific kind of protection to system resources

<p style="text-align: center;"><b>AUTHENTICATION</b></p> <p>The assurance that the communicating entity is the one that it claims to be.</p> <p><b>Peer Entity Authentication</b> Used in association with a logical connection to provide confidence in the identity of the entities connected.</p> <p><b>Data-Origin Authentication</b> In a connectionless transfer, provides assurance that the source of received data is as claimed.</p> <p style="text-align: center;"><b>ACCESS CONTROL</b></p> <p>The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).</p> <p style="text-align: center;"><b>DATA CONFIDENTIALITY</b></p> <p>The protection of data from unauthorized disclosure.</p> <p><b>Connection Confidentiality</b> The protection of all user data on a connection.</p> <p><b>Connectionless Confidentiality</b> The protection of all user data in a single data block</p> <p><b>Selective-Field Confidentiality</b> The confidentiality of selected fields within the user data on a connection or in a single data block.</p> <p><b>Traffic-Flow Confidentiality</b> The protection of the information that might be derived from observation of traffic flows.</p>	<p style="text-align: center;"><b>DATA INTEGRITY</b></p> <p>The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).</p> <p><b>Connection Integrity with Recovery</b> Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.</p> <p><b>Connection Integrity without Recovery</b> As above, but provides only detection without recovery.</p> <p><b>Selective-Field Connection Integrity</b> Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.</p> <p><b>Connectionless Integrity</b> Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.</p> <p><b>Selective-Field Connectionless Integrity</b> Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.</p> <p style="text-align: center;"><b>NONREPUDIATION</b></p> <p>Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.</p> <p><b>Nonrepudiation, Origin</b> Proof that the message was sent by the specified party.</p> <p><b>Nonrepudiation, Destination</b> Proof that the message was received by the specified party.</p>
---	--

# Authentication

- ▶ Concerned with assuring that a communication is authentic
  - ▶ In the case of a single message, assures the recipient that the message is from the source that it claims to be from
  - ▶ In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties
  - ▶ Two specific authentication services are defined in X.800 namely **peer entity authentication** and **data origin authentication**

# Access Control

- ▶ The ability to limit and control the access to host systems and applications via communications links
- ▶ To achieve this, each entity trying to gain access must first be indentified, or authenticated, so that access rights can be tailored to the individual

# Data Confidentiality

- ▶ The protection of transmitted data from passive attacks
  - ▶ Broadest service protects all user data transmitted between two users over a period of time
  - ▶ Narrower forms of service includes the protection of a single message or even specific fields within a message
- ▶ The protection of traffic flow from analysis
  - ▶ This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

# Data Integrity

- ▶ Can apply to a stream of messages, a single message or selected fields within a message
- ▶ **Connection-oriented Integrity service** deal with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering or replay.
- ▶ **Connection-less Integrity service** deals with individual messages without regard to larger context, generally provides protection against message modification only

# Non repudiation

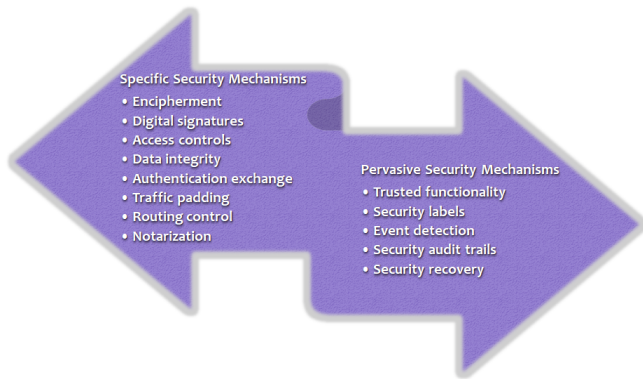
- ▶ Prevents either sender or receiver from denying a transmitted message
- ▶ When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- ▶ When a message is received, the sender can prove that the alleged receiver in fact received the message

# Availability Service

- ▶ Protects a system to ensure its availability
- ▶ This service addresses the security concerns raised by denial-of-service attacks
- ▶ It depends on proper management and control of system resources and thus depends on access control service and other security services



# Security Mechanisms (X.800)



# Security Mechanisms (X.800)..

## SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

### Encipherment

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

### Digital Signature

Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

### Access Control

A variety of mechanisms that enforce access rights to resources.

### Data Integrity

A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

### Authentication Exchange

A mechanism intended to ensure the identity of an entity by means of information exchange.

### Traffic Padding

The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

### Routing Control

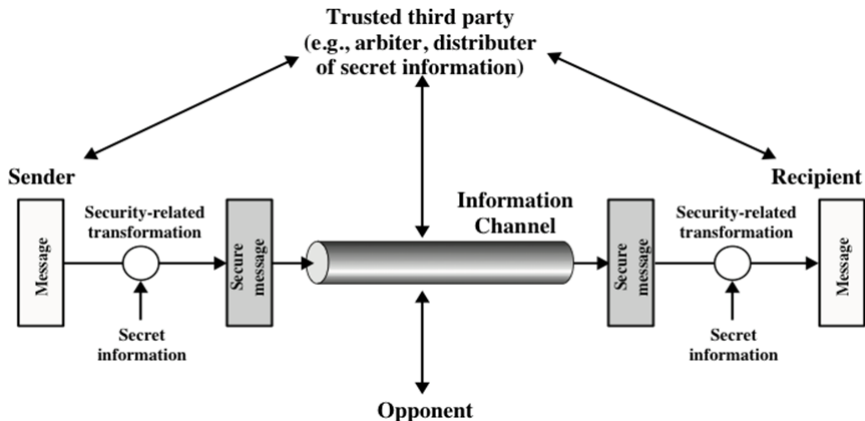
Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

### Notarization

The use of a trusted third party to assure certain properties of a data exchange.



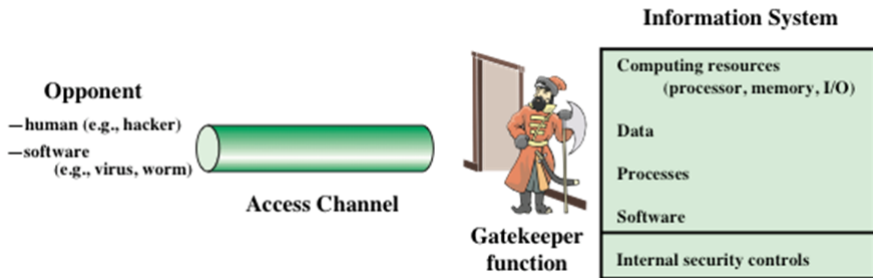
# Model for Network Security



## Model for Network Security...

- ▶ Design a algorithm for performing the security related transformation
- ▶ Generate the secret information to be used with the algorithm
- ▶ Develop methods for the distribution and sharing of the secret information
- ▶ Specify protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service

# Network Access Security Model



# Unwanted Access

- ▶ Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs such as editors and compilers
- ▶ Programs can present two kinds of threats:
  - ▶ **Information access threats:** Intercept or modify data on behalf of users who should not have access to that data
  - ▶ **Service threats** Exploit service flaws in computers to inhibit use by legitimate users

# References

1. Forouzan, Behrouz A. "Cryptography & Network Security. 2011."
2. Stallings, William. "Cryptography & Network Security: Principles and Practices. 7th Edition, 2017"

Last updated by S J Patel on January 8, 2024