Network Security (CC-603)

Unit- 1 (Network Security Fundamental)

- **Concept of Computer Security, Challeges of Computer Security**
  - **Concept of Computer Security**
    - ✓ Computer data travels from one computer to another, leaving the safety of its protected physical surroundings.
    - ✓ Once the data is sent, people with bad intentions could modify the data, either for misuse or for their own benefit.
    - ✓ Cryptography can reformat and transform data, making it safer during transmission between computers.
    - ✓ The technology of cryptography is based on the essentials of secret codes, augmented by modern mathematics that protects data in powerful ways.
    - ✓ Network Security deals with all aspects related to the protection of sensitive information assets existing on the network.
    - ✓ It covers various mechanisms developed to provide fundamental security services for data communication.
    - ✓ It describes the functioning of the most common security protocols employed at different networking layers from the application to the data link layer.
    - ✓ After going through this lecture, you will find yourself at an intermediate level of knowledge regarding network security.
  - **Needs for Network Security**
    - ✓ Unless properly secured, any network is vulnerable to malicious use and accidental damage. Hackers, disgruntled employees, or poor security practices within the organization can leave private data exposed, including trade secrets and customers' private details.
    - ✓ Losing confidential research can potentially cost an organization millions of dollars by taking away competitive advantages it paid to gain. Hackers stealing customers' details and selling them to be used in fraud create negative publicity and public mistrust of the organization.
    - ✓ The majority of common attacks against networks are designed to gain access to information by spying on the communications and data of users rather than damaging the network itself.
    - ✓ Attackers can also damage users' devices or manipulate systems to gain physical access to facilities, leaving the organization's property and members at risk of harm.
    - ✓ Competent network security procedures keep data secure and block vulnerable systems from outside interference, allowing users to remain safe and focus on achieving the organization's goals.
    - ✓ Network security protects the organization's reputation, ensuring clients and partners can interact confidently.

Prepared By :- Nilam Hariyani

Network Security (CC-603)

Unit- 1 (Network Security Fundamental)

- **Introduction CIA**

  - ✓ The general state in Computer Security has the ability to detect andprevent attacks and to be able to recover. If these attacks are successful as such then it has to contain the disruption of information and services and check if they are kept low or tolerable.

  - ✓ In order to fulfill these requirements, we come to the three mainelements which are confidentiality, integrity, and availability.

  - ✓ This definition introduces three key objectives that are at the heart of computer security, are explained below :

1. Confidentiality:

Confidentiality is the concealment of information or resources.Also, there is a need to keep information secret from other third parties that want to have access to it, so just the right people can access it.

Example in real life − Let"s say there are two people communicating via an encrypted email they know the decryption keys of each other and they read the email by entering these keys into the email program. If someone else can read these decryption keys when they are entered into the program, then the confidentiality of that email is compromised.

This term covers two related concepts:

1. Data Confidentiality:

The Data Confidentiality assures that private or confidential information is not made available or disclosed to unauthorized individuals (persons).

2. Privacy:

Privacy assures that individuals (any person) control or influence what information related to them, may be collected and stored, and by whom and to whom that information may be disclosed.

2. Integrity:

Integrity is the trust worthiness of data in the systems or resources by the point of view of preventing unauthorized and improper changes.

Generally, Integrity is composed of two sub- elements data-integrity, which it has to do with the content of the data and authentication which has to do with the origin of the data as such information has values only if it is correct.

Network Security (CC-603)

Unit- 1 (Network Security Fundamental)

Example in real life − Let‟s say you are doing an online payment of 5 USD, but your information is tampered without your knowledge in a way by sending to the seller 500 USD, this would cost you too much.

This term covers two related concepts:

1. Data Integrity:

The Data Integrity assures that information and programs are changed only in a specified and authorized manner.

2. System Integrity:

The System Integrity assures that a system performs its intended function in a proper manner, free from deliberate (intentionally) or inadvertent unauthorized manipulation of the system.

3. Availability:

Availability refers to the ability to access data of a resource when it is needed, as such the information has value only if the authorized people can access at right time. Denying access to data nowadays has become a common attack. Imagine a downtime of a live server how costly it can be.

Example in real life − Let‟s say a hacker has compromised a web server of a bank and put it down. You as an authenticated user want to do an e-banking transfer but it is impossible to access it, the undone transfer is a money lost for the bank.

The Availability assures that systems work promptly and service is not denied (rejected) to authorized users.

These three concepts are known as the “CIA triad”, that makes the following format for the Computer Security:

The three concepts joint the fundamental security objectives for both data and information with computing services.

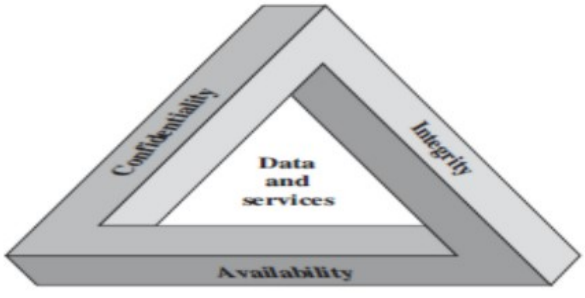


Figure 1.1 The Security Requirements Triad

Network Security (CC-603)

Unit- 1 (Network Security Fundamental)

- **Challenges of Computer Security**

1. Evolving Threat Landscape:

The nature of cyber threats is constantly changing. New types of malware, ransomware, and phishing attacks are developed regularly, making it challenging to keep up with and defend against the latest threats.

2. Human Error:

Users are often the weakest link in security. Phishing attacks, weak passwords, and accidental sharing of sensitive information can compromise security.

3. Advanced Persistent Threats (APTs):

APTs are long-term targeted attacks aimed at stealing sensitive information. They often involve sophisticated techniques that can evade traditional security measures.

4. Zero-Day Vulnerabilities:

These are vulnerabilities that are unknown to the software vendor and do not have a patch available. Exploiting these vulnerabilities can lead to significant security breaches.

5. Resource Constraints:

Many organizations lack the necessary resources, both in terms of budget and skilled personnel, to implement and maintain robust security measures.

6 Complexity of IT Environments:

Modern IT environments are complex, with a mix of legacy systems, cloud services, mobile devices, and IoT devices. Ensuring security across such diverse environments is challenging.

7. Regulatory Compliance:

Organizations must comply with various regulations and standards (e.g., GDPR, HIPAA, PCI-DSS) which can be complex and costly to implement.

8. Data Privacy and Protection:

Protecting the privacy of user data and ensuring data integrity is crucial. Data breaches can lead to significant legal and financial repercussions.

9. Insider Threats::

Employees or contractors with access to sensitive information can pose a significant risk if they misuse their access, either intentionally or unintentionally.

- **The OSI Security Architecture**

✓ The OSI (Open Systems Interconnection) Security Architecture is a framework designed to provide a standardized approach to network security. It's based on the seven-layer OSI model, which is a conceptual framework for understanding network communication.

✓ **Key Concepts in OSI Security Architecture:**

1. **Security Attacks:**
   - **Passive Attacks:** Eavesdropping or traffic analysis.
   - **Active Attacks:** Modification or impersonation.
2. **Security Services:**
   - **Confidentiality:** Ensuring data remains secret.
   - **Integrity:** Ensuring data is not altered.
   - **Availability:** Ensuring data is accessible when needed.
   - **Authentication:** Verifying the identity of a user or device.
   - **Non-repudiation:** Preventing a party from denying their involvement in a transaction.
3. **Security Mechanisms:**
   - **Encryption:** Transforming data to make it unreadable.
   - **Digital Signatures:** Verifying the authenticity and integrity of data.
   - **Access Control:** Limiting access to resources.
   - **Data Integrity:** Ensuring data has not been altered.

OSI Security Architecture and the OSI Model:

The OSI Security Architecture applies these concepts to each layer of the OSI model:

Network Security (CC-603)

Unit- 1 (Network Security Fundamental)

- **Physical Layer:**
  - **Security Services:** None specific to this layer.
  - **Security Mechanisms:** Physical security measures (e.g., locks, guards).
- **Data Link Layer:**
  - **Security Services:** Data integrity, authentication.
  - **Security Mechanisms:** Error detection codes, link encryption.
- **Network Layer:**
  - **Security Services:** Confidentiality, authentication, access control.
  - **Security Mechanisms:** Routing protocols, virtual private networks (VPNs).

- **Transport Layer:**
  - **Security Services:** Confidentiality, integrity, end-to-end error control.
  - **Security Mechanisms:** Encryption, checksums.
- **Session Layer:**
  - **Security Services:** Authentication, access control.
  - **Security Mechanisms:** Session keys, mutual authentication protocols.
- **Presentation Layer:**
  - **Security Services:** Data encryption, data compression.
  - **Security Mechanisms:** Encryption algorithms, data compression techniques.
- **Application Layer:**
  - **Security Services:** All security services.
  - **Security Mechanisms:** All security mechanisms.

Network Security (CC-603)

Unit- 1 (Network Security Fundamental)

OSI Layer	Purpose	PDU	Device	Troubleshoot
Application	Interface (API)	Message	-	Wireshark
Presentation	Formatting, Encryption, Compression	Message	-	Wireshark
Session	Authentication, Authorization	Message	Gateway	NSLOOKUP, NBTSTAT, Wireshark
Transport	Reliability	Segment (TCP), Datagram (UDP)	Firewall	TELNET, NETSTAT, Wireshark
Network	Addressing, Routing	Packet	Router	IPCONFIG, PING, TRACERT, Wireshark
Data Link	Logical Link Control, Media Access Control	Frame	Switch, Bridge, AP	Lights on device, ARP, Wireshark
Physical	Transmission	Bit	Hub, NIC, Cable, Wireless	Lights on device

Importance of the OSI Security Architecture:

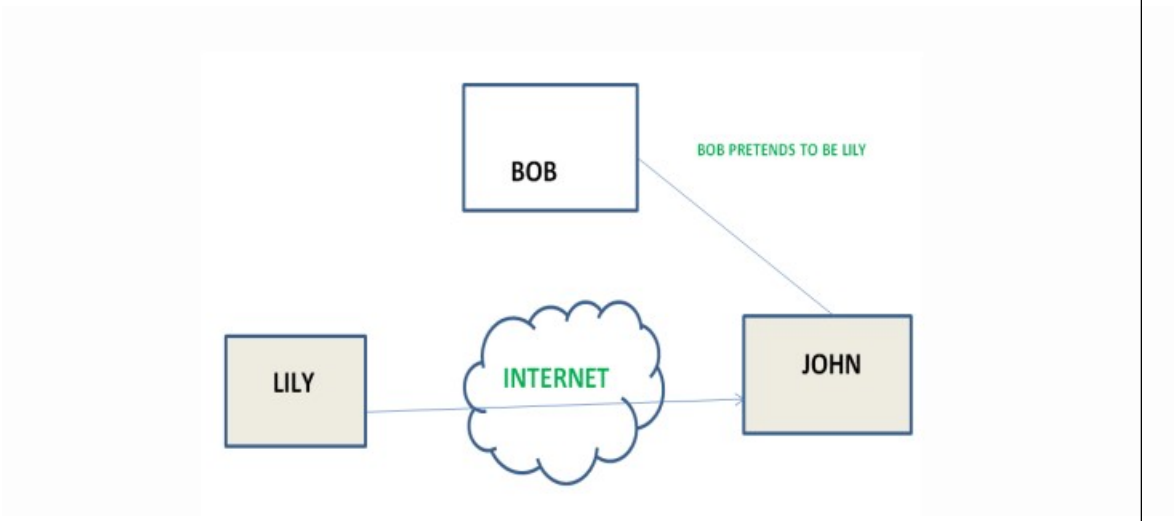
- **Standardization:** Provides a common framework for understanding and implementing network security.
- **Layered Approach:** Allows for security measures to be applied at different levels of the network.
- **Comprehensive:** Covers a wide range of security concerns, from physical security to application-level security.

- **Types of Security attacks | Active and Passive attacks**

  - Active attacks:
  - ✓ An Active attack attempts to alter system resources or effect their operations.
  - ✓ Active attack involve some modification of the data stream or creation of false statement.

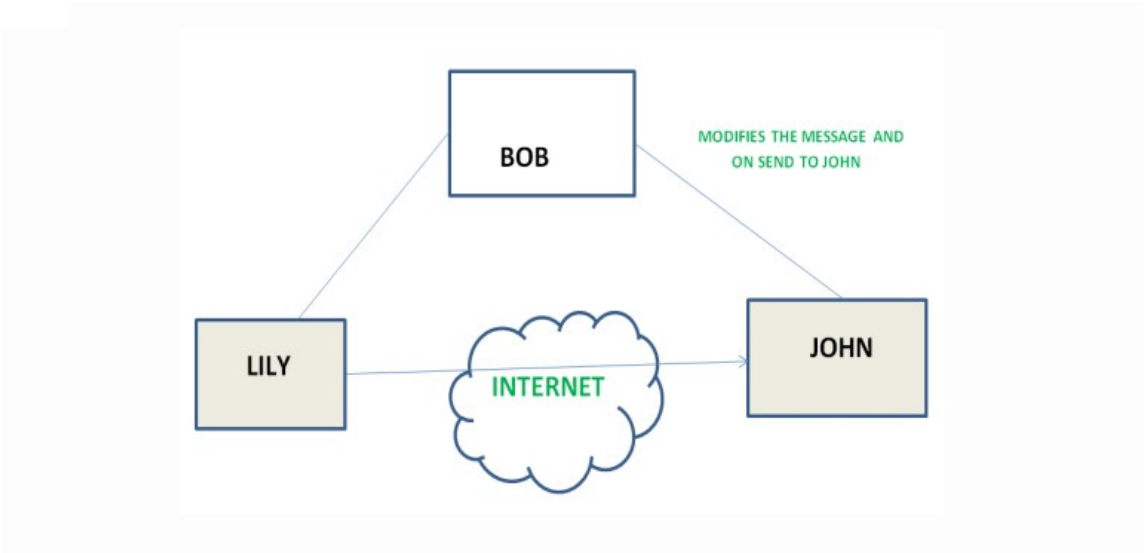
  - Types of active attacks are as following:

  1. Masquerade –
  - ✓ Masquerade attack takes place when one entity pretends to be different entity.
  - ✓ A Masquerade attack involves one of the other form of active attacks.



2. Modification of messages:-

- ✓ It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. • For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.

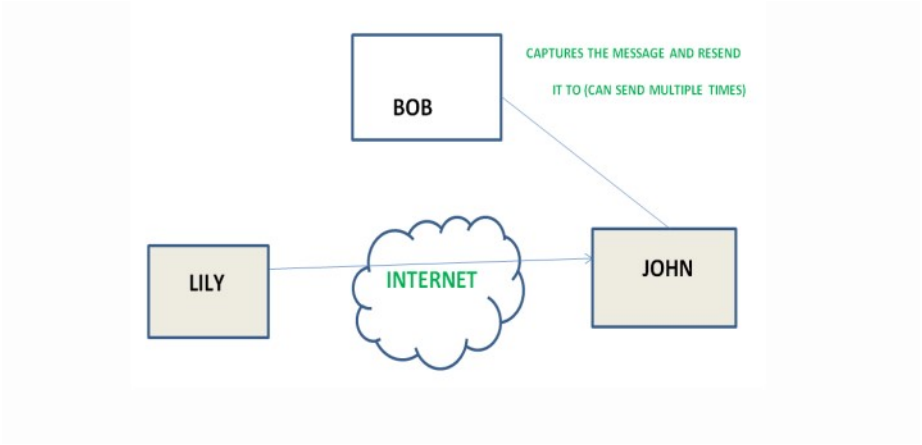


3. Repudiation

- ✓ This attack is done by either sender or receiver. • The sender or receiver can deny later that he/she has send or receive a message. • For example, customer ask his Bank “To transfer an amount to someone” and later on the sender(customer) deny that he had made such a request. This is repudiation.

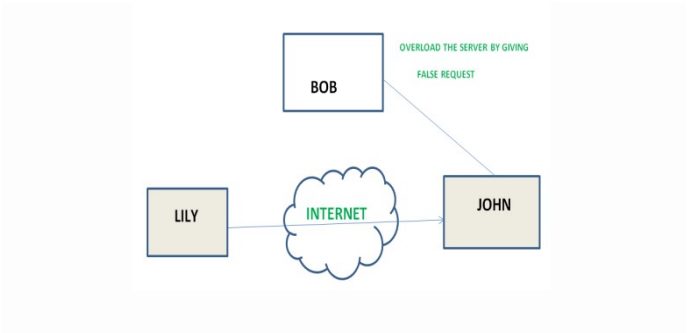
4. Replay

- ✓ It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.



5. Denial of Service

- ✓ It prevents normal use of communication facilities.
- ✓ This attack may have a specific target.
- ✓ For example, an entity may suppress all messages directed to a particular destination.
- ✓ Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



Network Security (CC-603)

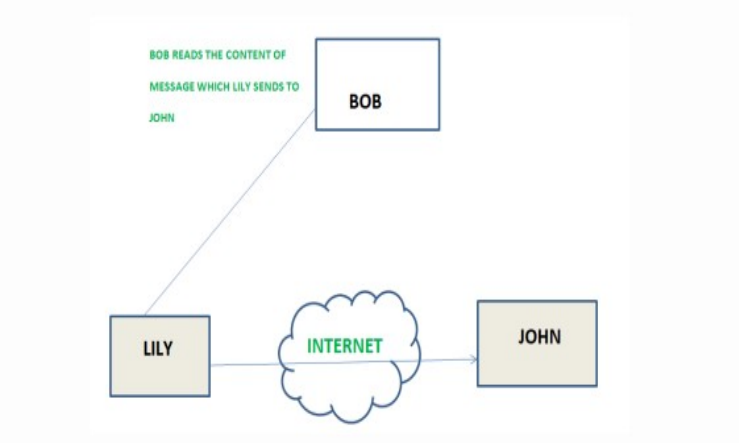
Unit- 1 (Network Security Fundamental)

- **Passive attacks**

  - ✓ A Passive attack attempts to learn or make use of information from the system but does not affect system resources.
  - ✓ Passive Attacks are in the nature of eavesdropping on or monitoring of transmission.
  - ✓ The goal of the opponent is to obtain information is being transmitted.
  - ✓ Types of Passive attacks are as following:

1. **The release of message content**

   - ✓ Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information.
   - ✓ We would like to prevent an opponent from learning the contents of these transmissions.

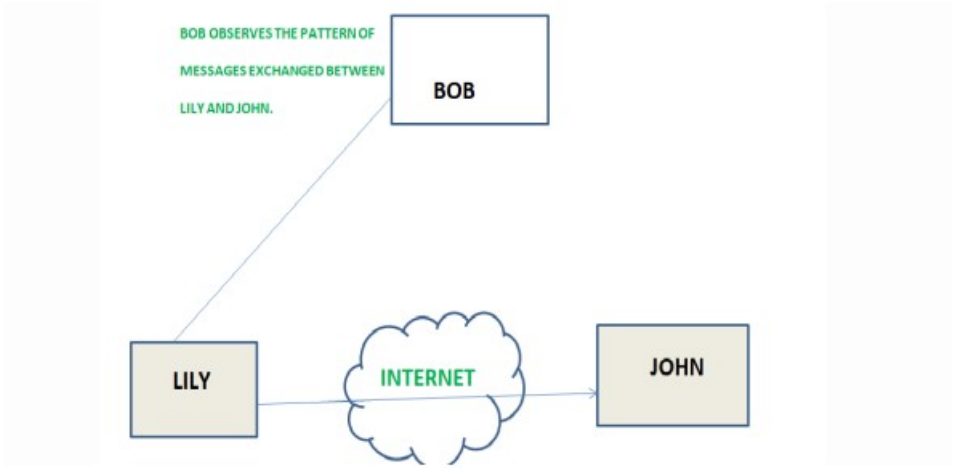


2. **Traffic analysis**

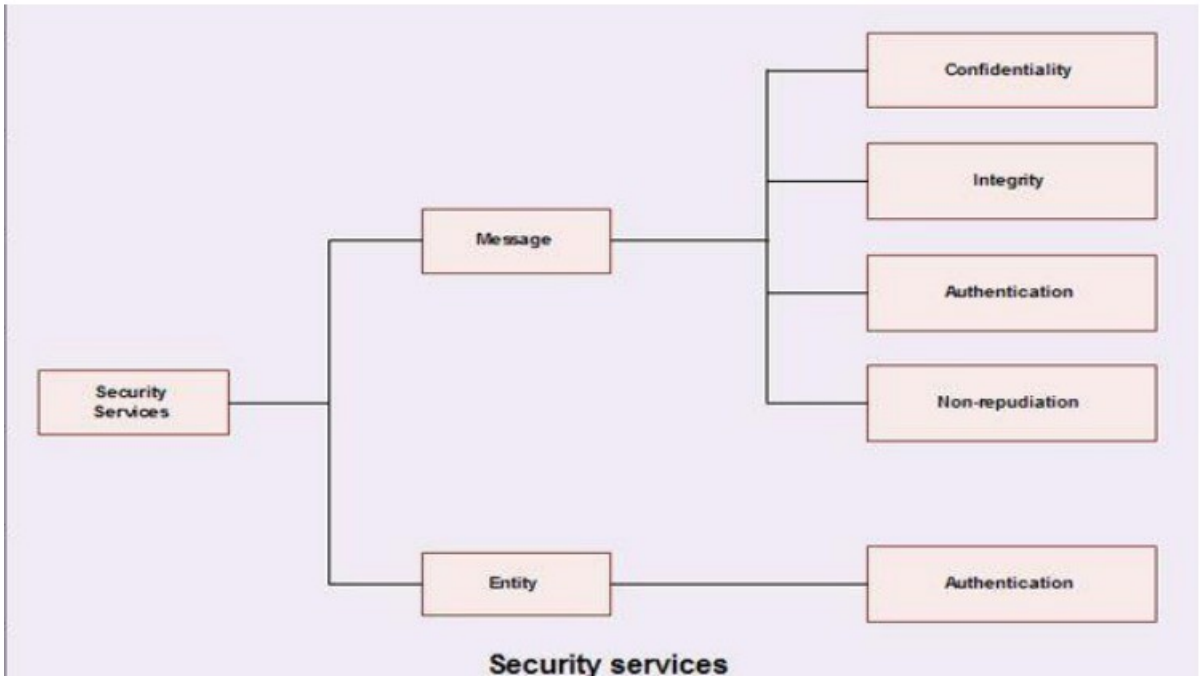
   - ✓ Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.
   - ✓ The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged.
   - ✓ This information might be useful in guessing the nature of the communication that was taking place.

Network Security (CC-603)

Unit- 1 (Network Security Fundamental)



Security Services



Security services

Network Security (CC-603)

Unit- 1 (Network Security Fundamental)

- **Authantication(પ્રમાણીકરણ)**

  - ✓ The assurance that the communicating entity is the one that it claims to be

    - ➢ **Peer Entity Authentication():-**
      Used in association with a logical communication to provide confidence in the identity of the entities connected.

    - ➢ **Data Origin Authantication (મૂળ પ્રમાણીકરણ):-**
      In a connection less transfer, provide assurance that the source of received data is as claimed.

    - ➢ **Access Control(વપરાશ ડનયાંત્રણ):-**
      The prevention of unauthorized use of a resource (i.e This service controls who can have access to a resource, under what condition access can occur, and what those accessing the resource are allowed to do.)

- Data Confidentiality(ડેટા ગોપનીયતા):

  - ✓ The Protection of data from unauthorized disclosure.

    - ➢ **Connection Confidentiality:-**
      the Protection of all user data on a connection.

    - ➢ **Connectionless Confidentiality:-**
      The protection of all User data in a single data block.

    - ➢ **Selective-Field Confidentiality:-**
      the Confidentiality of selected fields within the user data on a connection or in a single data block.

    - ➢ **Traffic flow Confidentiality:-**
      The Protection of the Information that might be derived from observation of traffic flows.

- Data Integrity(માડહતી સાંકલતતા):

  - ✓ The assurance that data receives are exactly as sent by an authorized entity (i.e., contain no modification , insertion , deletion or replay).

- Connection Integrity with Recovery:
  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.

- **Connection Integrity without Recovery:**
  As above , but provides only detection without recovery.

- **Connectionless Integrity :**
  Provides for the integrity of a single connection less data block and may take the form of detection of data modification. Additionally, limited form of replay detection may be provided.

- **Selective field Connectionless Integrity**
  Provide for the integrity of selected fields within a single connection less data block; take the form of determination of whether the selected fields have been modified.

- **Non Repudiation (ડિન રડિયો):**

  - ✓ Provides protection against denial by one of the entities involved in a communication of having participated in all or part of a Communication.

  - **Non Repudiation , Origin(નોન ડરિીડડએશન, મૂળ):**
    Proof that the message was sent by the specified party.

  - **Non Repudiation , Destination(Rep અસ્વીર્ાર, લક્ષ્ય) :**
    Proof that the message was received by the specified party.

- **A MODEL FOR NETWORK SECURITY :-**

  - ✓ A security-related transformation on the information to be sent.
  - ✓ Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

Network Security (CC-603)

Unit- 1 (Network Security Fundamental)

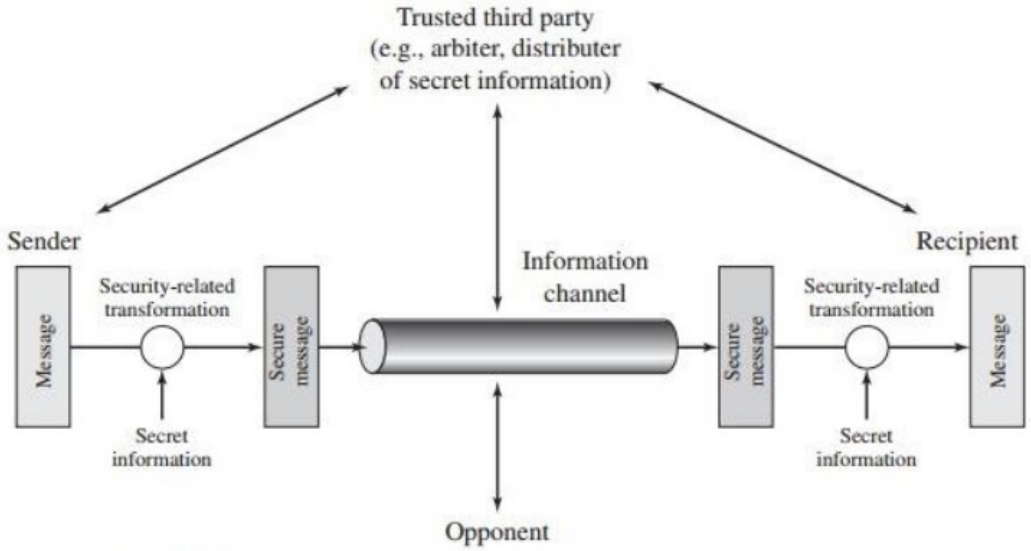


Figure 1.4 Model for Network Security

- ✓ Some secret information shared by the two principals and, it is hoped, unknown to the opponent.
- ✓ An example is an encryption key used in conjunc-tion with the transformation to scramble the message before transmission and unscramble it on reception.
- ✓ A trusted third party may be needed to achieve secure transmission.
- ✓ For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent.
- ✓ Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.
- ✓ This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a 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.