Network Security

Major Standardization Bodies

1. ***IETF:*** The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. Standards are available in the form of RFCs (Request for Comments).
2. ***ITU-T:*** ITU is the United Nations specialized agency for information and communication technologies. ITU-T is one of the three sectors of the International Telecommunication Union (ITU); it coordinates standards for telecommunications.
3. ***NIST:*** National Institute of Standards and Technology (NIST) is the US federal technology agency that works with industry to develop and apply technology, measurements, and standards.
4. ***ISO:*** The International Organization for Standardization (ISO) is a non-government international standard-setting body composed of representatives from various national standards organizations. It works in several areas including networking and security.

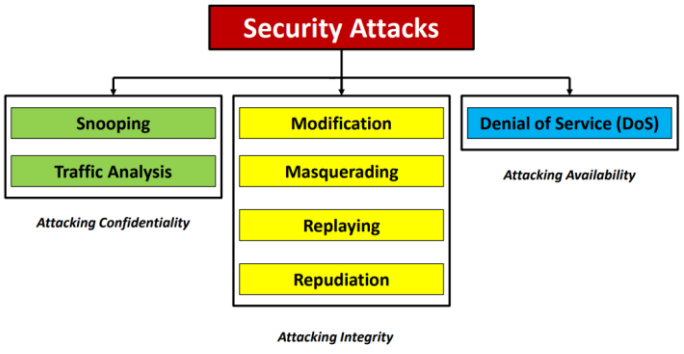
Information Security

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 (includes hardware, software, firmware, information/data, and telecommunications).

The OSI Security Architecture

1. Network Security needs some systematic way of defining the security requirements and approaches to meet them.
2. ITU-T Recommendation X.800, defines a systematic approach for this purpose focusing on the following three aspects:
    a. ***Security Attack:*** Any action that compromises the security of information owned by an organization.
    b. ***Security Mechanism***: A process that is designed to detect, prevent, or recover from a specific security attack.
    c. ***Security Service:*** A service that makes use of one or more security mechanisms and provides specific kind of protection to the system.

Security Attacks



Snooping	Data is intercepted by an unauthorized person. E.g. Tapping.
Traffic Analysis	May be the data is masked, so no information can be extracted but some patterns like - sender, receiver, message length, time of the message etc. can be extracted to make intelligent guesses.
Modification	Some portion of a legitimate message is altered or the message is delayed.
Masquerading	One entity pretends to be a different entity. E.g. Hoax bank sites.
Replaying	Subsequent retransmission of a captured message to produce an unauthorized effect. E.g. Bill payment fake reminders with fake links
Repudiation	Sender denies that it sent the message or the receiver denies that it received the message.
Denial of Service	Slowing down or totally interrupt the service of the system. E.g. multiple requests to bring an exam result server down.

Passive Attacks – The attacker's goal is to just obtain the information. The attack does not harm the system.

Active Attacks **–** The attacker changes the data or harms the system.

Security Mechanisms

Encipherment	The use of mathematical algorithms to transform data into a form that is not readily intelligible.
Digital Signature	A data unit that allows a recipient of the data unit to prove the source.
Access Control	Access rights to the resources restrained.
Data Integrity	A mechanism to append a check value with the data. Receiver calculates check value on the data and compares it with the received one.
Authentication Exchange	Two entities exchange the messages to prove their identities to each other.
Traffic Padding	Insertion of bogus data to thwart the traffic analysis.
Routing Control	Discretionary selection of routes between sender and receiver based of the security risks.
Notarization	Trusted third party assures the information exchange.

Security Services

Authentication	The assurance that the communicating entity is the one that it claims to be. 1. Peer Entity: Sender/receiver authentication in connection-oriented communication. 2. Data Origin: Data source authentication in connectionless communication.
Access Control	The prevention of unauthorized access of a resource. Access definition could be broad here and can involve – read, write, modify, execute etc.
Data Confidentiality	The protection of data from unauthorized disclosure. X.800 is very broad and encompasses confidentiality of the whole

	message or the part of the message and also protection against traffic analysis.
Data Integrity	he assurance that data received is exactly as sent by an authorized entity (i.e. It contains no modification, insertion, deletion, or replay).
Non-Repudiation	Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication

Availability & Availability Service

Availability: X.800 defines availability to be the inherent property of a system. A system resource must accessible and usable upon demand by an authorized entity. A variety of attacks can result in the loss or reduction in availability.

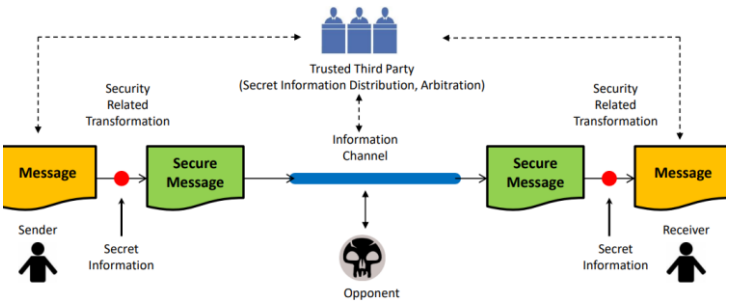
The availability service addresses the security concerns raised by Denial-of-Service attacks. It can be treated as sixth type of security service.

Security Mechanisms and Services

Security Service is a processing or communication service that is provided by a system to give a specific kind of protection to the system resources. Security services are implemented by security mechanisms. [RFC-4949]. A mechanism or combination of mechanisms are used to provide a service. Also a mechanism can be used in one or more services.

Security Service	Security Mechanism
Data Confidentiality	Encipherment, Routing Control
Data Integrity	Digital Signature
Non- Repudiation	Digital Signature, Notarization

A Model for Network Security



1. A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the sender and receiver.
2. An opponent may present a threat to the confidentiality of the message that is being transmitted.
3. Using a secret information, sender secures the original message (encrypted or ciphered) and using the same secret information receiver recovers the original message (decrypted or deciphered).
4. A trusted third party distributes the secret information to both the sender and receiver.

The Network Security

Model for the Network Security on the previous slide 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 ***(ENCRYPTION/ DECRYPTION).***
2. Generate the secret information to be used with the algorithm ***(KEY MANAGEMENT).***
3. Develop methods for the distribution and sharing of the secret information ***(KEY DISTRIBUTION).***
4. Specify a protocol to be used by the two users that makes use of the security algorithm and the secret information to achieve a particular security service ***(IMPLEMENTATION).***

Techniques to Implement Security Mechanisms

Cryptography: in Greek it means "secret writing". In the network security it means the science of transforming the messages to make them secure and immune to attacks.

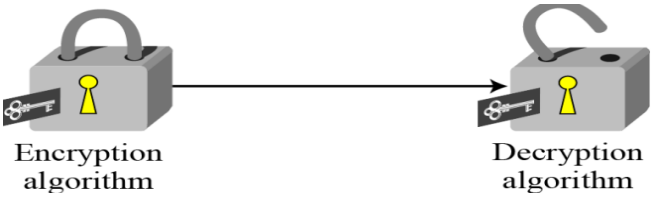
a. Symmetric-Key Encipherment
b. Asymmetric-Key Encipherment
c. Data Integrity
d. Mutual Trust

Steganography: in Greek it means "covered writing". In contrast with cryptography, it means concealing the message itself by covering it with something else. Example: A letter is written on the paper using onion juice or ammonia salts which would not be visible unless exposed to heat, message hidden in paintings etc.

Symmetric-Key Encipherment

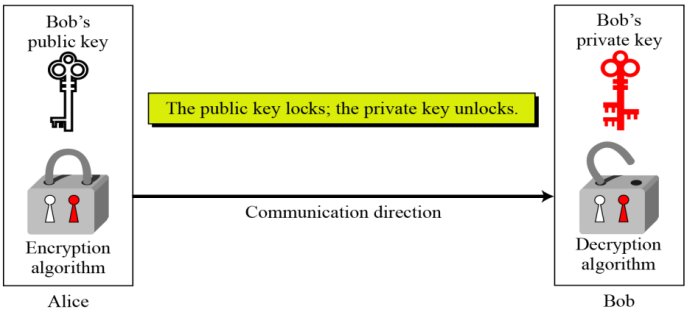
Sender encrypts the message using an encryption algorithm and the receiver decrypts the message using a decryption algorithm. Symmetric-Key Encipherment uses a single secret key for both encryption and decryption.

It is analogous to the sender puts the message in a box and locks the box with a shared key. The receiver opens the box with the same shared key and gets the message.



Asymmetric-Key Encipherment

To send a secure message, the sender first encrypts the message using receiver's public key. To decrypt the message, the receiver uses its own private key.

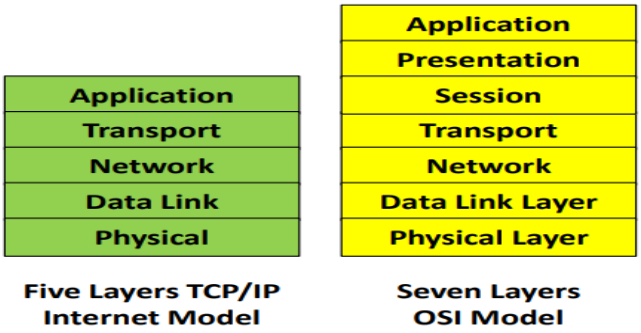


Data Integrity and Mutual Trust

Data Integrity: Different cryptographic techniques to ensure data integrity. E.g. Hashing and Message digest.

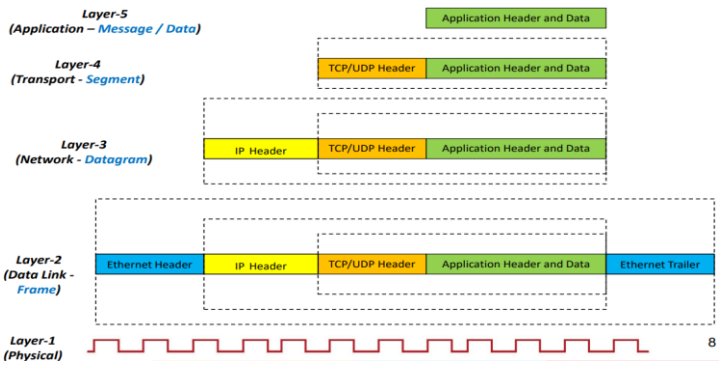
Mutual Trust: Different methods for key generation and distribution. Entity authentication and notarization methods.

Computer Networks: A Layered Architecture

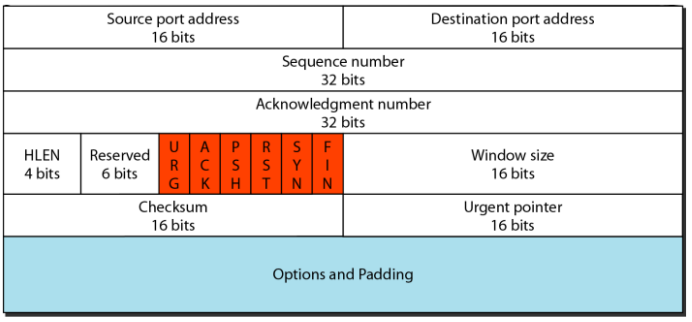


1. Similar to the airline functionality, a modern computer network can be designed in a layered architecture.
2. A layer can be implemented in software, in hardware, or in a combination of the two. An application (e.g. HTTP) is usually implemented in software, whereas physical layer and data link layers are implemented in hardware (e.g. network interface cards).
3. Rules for the two layers to communicate between two peer entities (hosts) is called a protocol. When taken together, the protocols of the various layers are called the protocol stack.

Networking Packetization



How to Analyze Packets?



An engineer captured some transmission using a packet capture tool. The hex dump of a TCP segment starting from the TCP header is: **00 19 05 BE 05 59 54 39 0D 57 59 A9 50 18 FF FF 7B 2E 00 00** 33 35 34 20 67 6F 20 61 68 65 61 64 0D 0A 2E 0D 0A. The TCP header is without the optional data. What is being conveyed through this TCP segment?

1. ***What is the source port address?***
   The 16 bits for source port address are 00 19 in hexadecimal that is 25 in decimal.
2. ***So, who is sending this message?***
   SMTP Server.
3. ***How do we know that?***
   TCP port 25 is a well known port for SMTP server.
4. ***What is being conveyed by the TCP segment?***
   The data after 20 bytes of TCP header: 33 35 34 20 67 6F 20 61 68 65 61 64 0D 0A 2E 0D 0A
5. ***But what is it?***
   We know SMTP is a ASCII based protocol. The equivalent ASCII text is 354 go ahead CRLF.CRLF.

Question: Few bytes are captured during some transmission using a packet capture tool like Wireshark. The hex dump of a IPv4 datagram starting from the IPv4 header is: **45 00 00 49 24 4d 40 00 80 06 30 67 c0 a8 01 04 d9 0c**

0b 42 05 be 00 19 0d 57 59 60 05 59 54 29 50 18 ff 3c 1c f1 00 00

4d 41 49 4c 20 46 52 4f 4d 3a 20 3c 78 78 78 78 78 78 40 78 78 78 78 78 2e 63 6f 2e 75 6b 3e 0d 0a.

The IP and TCP headers are without any optional data. Answer the following questions:

1. What are the source and destination IP addresses? Answer in dotted decimal notation.
2. From which byte do we know that it is TCP and how?
3. What are the source and destination port numbers?
4. What application protocol data is present in the datagram?
5. What is the direction of the data? Server to client or client to server?
6. What application message is being conveyed?

Cryptography Terminology

1. ***Plaintext*** – An original message in its 'as-it-is' form.
2. ***Ciphertext*** – Coded message. Cannot be understood just by reading it.