Network Security

Types of Attacks

With respect to communication of information across a networks, following can be types of attacks:

1. Disclosure

It is the release of message content to any person or process not possessing the appropriate cryptographic key.

2. Traffic Analysis

Discovery of traffic pattern between two parties in a connection oriented application. The frequency and duration of such connection can be identified and the lengths and the numbers of the message can be determined depending upon which the message can be decrypted.

3. Masquarade

Insertion of messages into a network from a ~~fraudu~~ fraudulent source. This includes creation of message by an opponent that are supposed to come from authorized entities. It also includes ~~fraud~~ fraudulent acknowledgment of message by someone other than the message receipient.

4. Content Modification

The changes in the content of the message including insertion, deletion, transposition or modification.

5. Sequence Modification

Any modification in the sequence of the message between the parties including insertion, deletion or re-ordering

6. Timing Modification

It includes delay or replay of the message in connection oriented application. An entire message or a portion could be replayed of some previous valid session or invalid message in the sequence could be delayed or replayed.

7. Non-Repudiation

Denial of receipt of message by destination or denial of transmission by the source

Security Models

For all kinds of security protocol, there are some kinds of issues that we need to consider which means that with some variation, a packet from an appropriate layer is taken by all the security protocols and a new package is created which is authenticated and encrypted. For this purpose, we first need to create a MAC and then we need to encrypt the message and the MAC as well. The most common structure

of security protocol is given below:

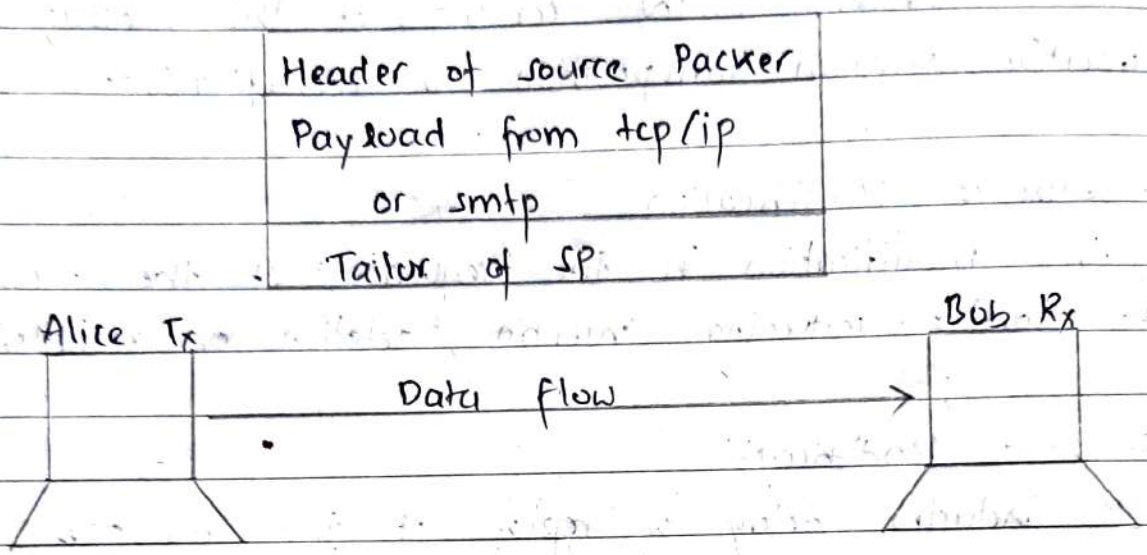


Fig: General security Model

There are 3 fundamental aspects of providing information security in internet application. They are:

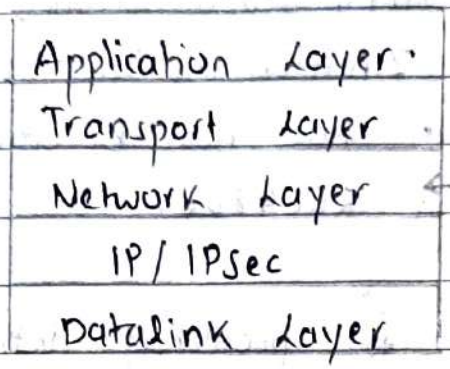
1. Integrity
2. Authentication
3. Key Management

Information security maybe provided at different layers in the internet communication protocols. In the network layer, we can use IPsec (IP security) for session layer. SSL or TLS can be used and we can embed security in the application itself using PGP (Pretty Good Privacy) or S/MIME can be used.

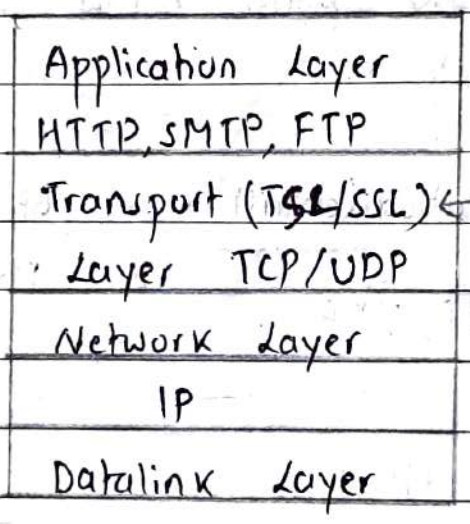
Consider the different types of security provided in

different layers shown in the diagram below:

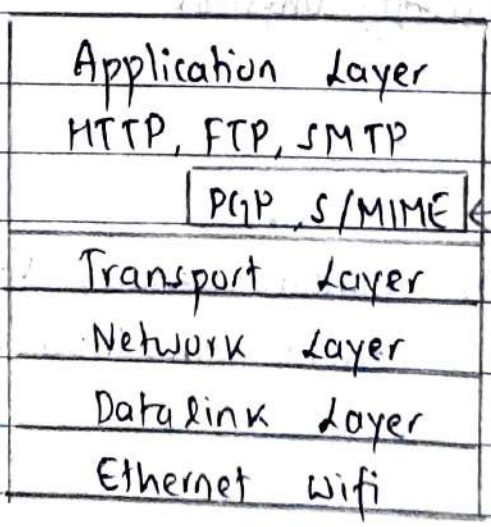
a)



b)



c)



Email Security (PGP)

PGP stands for Pretty Good Privacy which was originally developed by Phill Zimmerman in 1991. It was developed as open PGP and it has now become an open source standard described in RFC4880.

PGP is widely used for protecting data in long term storage. It is design to create authenticated messages and confidential emails. The figure below shows the position of PGP in TCP/IP protocol.

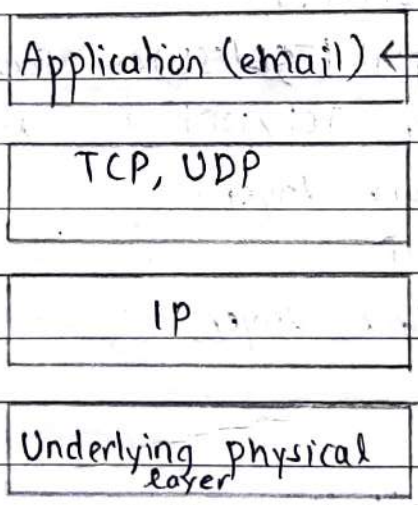


fig: Position of PGP in TCP/IP protocol

PGP can provide various services based on the requirements of the user and email can be used one or more of the services.

1. Plain text
   ↳ It is the simplest case to send the email. (no services used).

2. Message Authentication

→ Probably the next environment is to let the sender sign the message so that it can be authentic message which maybe verified by the user.

3. Compression

→ A further improvement is to compress the message and the message digest to make the packet more compact This has no security benefit but it eases the traffic.

4. Confidentiality

→ In email, confidentiality can be achieved by using symmetric key encryption with a one time session key. Pgp may use CAST 128 or IDEA or AES/DES with CAST 128 as their default choice for block-cipher algorithm.

→ A 128-bit encryption called the session key is generated for each email separately and encrypted with receiver public key using RSA, Diffie-Hellman and El-gamal.

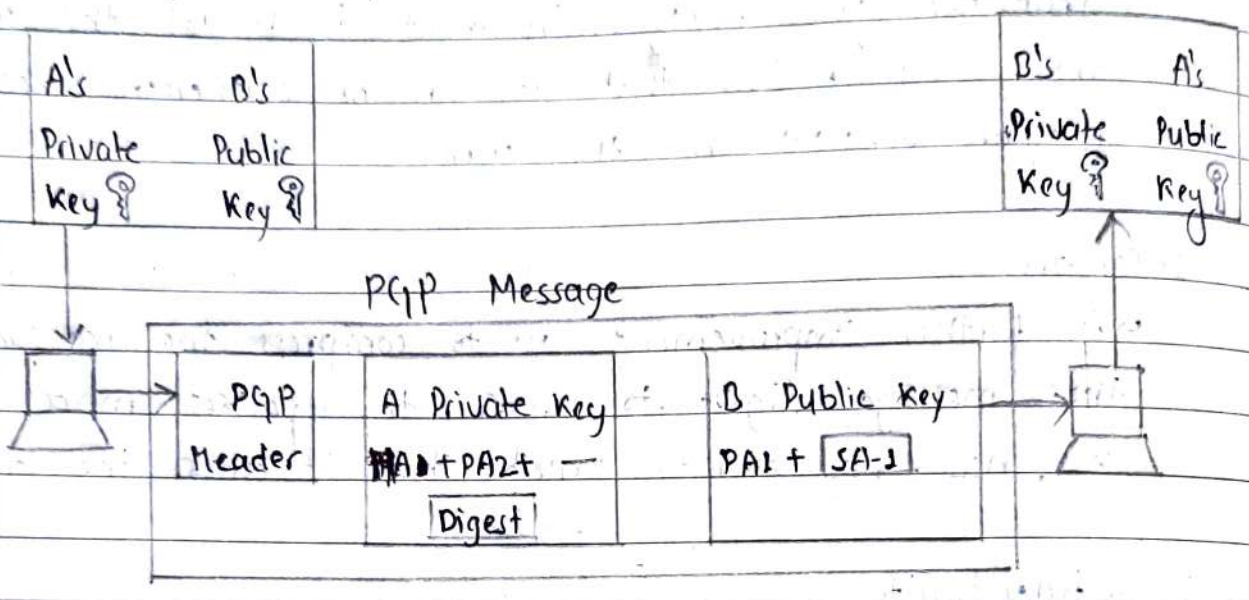
5. Code Conversion

→ Pgp uses RADIX-64 conversion for those conversion that are not defined in ASCII set. Each character to be sent is converted to RADIX 64 code after encryption.

6. Segmentation

→ Pgp allows segmentation after the code conversion to make each transmitted unit to the uniform size by the

underlying email protocol.



PA1: Public Key Algorithm 1 for encryption session key.
PA2: Public Key Algorithm for encrypting message digest
SA: Symmetric key Algorithm for encrypting message & digest
HA: Hash Algorithm for creating message digest.

Fig: Applying PGP to email message

1. At sender side:

The sender creates a session key (symmetric encryption/decryption) and concatenates with identity to the algorithm which will use this key. The result is encrypted with receiver's public key. This consists of 3 pieces of information:

a) Session Key
b) Symmetric Key algorithm to be used later.
c) Asymmetric Key algorithm used for this part.

A) The sender authenticates message using P-K signature algorithm and encrypts with sender's private key. This part of message contains the signature and two extra piece of info (Encryption algorithm and Hash algorithm identifier).

B) Alice / the sender concatenate these pieces of information created above with the message (email) and encrypts the whole thing using session key created at step 2.

C) Sender combines the result of step (A) & (B) and sends them to receiver adding appropriate header.

The algorithm used in PGP is given below. The new algorithm maybe added continuously.

Algorithm	ID	Description
Public Key	1	RSA (encryption & signing)
	2	RSA (encryption only)
	3	RSA (signing only)
	17	DSA (signing)
Hash Function	1	MD-5
	2	SHA-1
	3	RIPE-MD
Encryption	0	No encryption
	1	IDEA
	2	3-DES
	9	AES

Key-Ring

→ Sender needs to manage a key ring in case of sending message to many people.

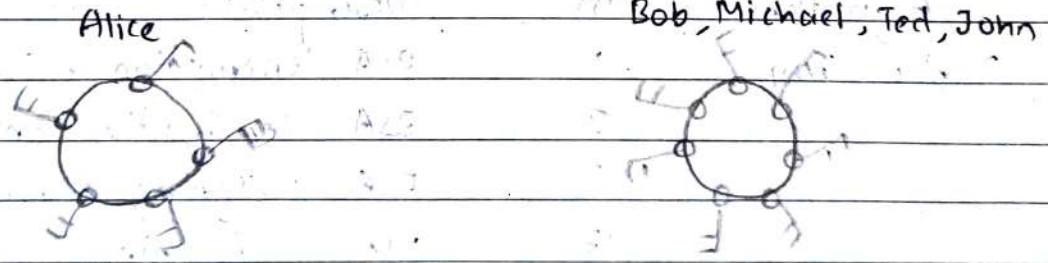
→ Sender's key ring of public key consists of keys belonging to each person whom sender needs to correspond.

→ In addition, the sender needs a private/public key ring for changing pair of key time to time correspond to different group of people.

→ Sender may wish to use a different key pair for different group.

→ Hence, each user needs to have two sets of rings.

1. A ring of private/public key &
2. A ring of public key of other people.



→ Each person in the ring can keep more than one public key for other person. Since everyone can have more than one public key, two cases may arise:

1. Person needs to send message to another in community. S/he uses receivers public key to encrypt newly created session key. S/he encrypts the message and signs the digest with session key.

2. A person receives a message from the member in the community. S/he uses private key to decrypt the session key. Using this session key, decrypts the message and digest & finally uses the public key to verify the language.

Secure Electronic Transaction (SET)

↳ It is a set of communication protocol that is used specially for electronic transaction over unsecure network specially the internet.

↳ It is a set of security protocol and formats that enables the users to employ existing credit card payment infrastructure on an open network in a secure fashion.

↳ SET was developed by SET consortium established in 1996 intending to become the De-facto standard payment method in the internet between the buyers, purchants and credit card companies.

↳ SET incorporates the following features to meet the business requirements.

1. Confidentiality
2. Account Authentication of the user
3. Merchant Authentication

↳ SET includes a cardholder, a merchant and issuer, a payment gateway and certification authority.

Process of Transaction

↳ Both the cardholder and merchant must register with certification Authority (CA) before they can buy or sell anything in the internet.

↳ The cardholder and the merchant start transaction which involves 9 basic steps which is listed below:

1. Customer browses the website and decide what to purchase.
2. Customer sends order and payment information. The message sent has two parts, purchase order and card information.
3. Merchant forwards the card information to the bank.
4. Merchant bank checks with the issuer for payment authentication.
5. Issuer sends the authorization to merchant bank.
6. The merchant's bank sends authorization to merchant.
7. The merchant completes the order and sends confirmation to the customer.
8. The merchant captures the transaction from their bank.
9. Finally, the issuer prints credit card bill or invoice to the customer.

Secure Socket Layer (SSL)

↳ SSL is a transport layer that provides N-N security service for application that uses a reliable transport layer protocol such as TCP (Transmission Control Protocol).

↳ When a customer shops online, following security services are desire.

1. Entity Authentication
2. Message Integrity
3. Confidentiality.

↳ Two protocols dominantly used today for providing security at transport layer are:

1. SSL
2. TSL.

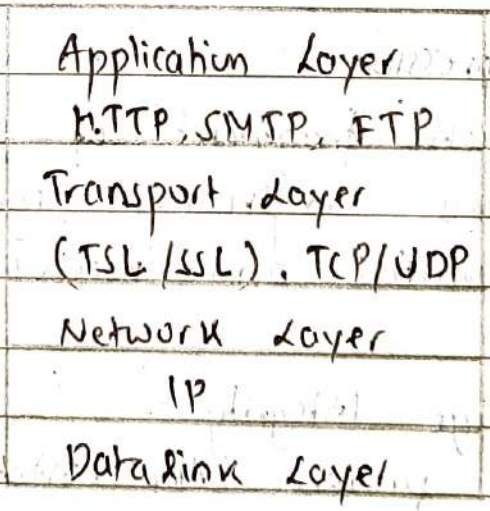


Fig: Location of TSL/SSL.

SSL Services

→ It is designed to provide security and compression services to the data generated from application layer.
→ Typically, SSL can receive data from any application layer protocol. But it receives typically from HTTP.
→ The data received from application are optionally compressed, signed and encrypted.
→ The data is then passed to TCP layer.
→ SSL provides services on data received from application layer such as:

1. Fragmentation
   - At first, SSL divides the data block into blocks of sizes, 2^{14} bytes or less.

2. Compression
   Each fragment of data is compressed using lossless compression negotiated between the transmitter and receiver. This service is optional.

3. Message Integrity
   To preserve the integrity of data, SSL uses keyed hash function to create a MAC.

4. Confidentiality
   The original data and MAC are encrypted using symmetric key ~~entry~~ cryptography to ensure confidentiality.

5. Framing

A header is added to the encrypted payload which is then passed to a reliable transport layer protocol such as TCP.