Electronic Mail Security

1) PGP

PGP stands for pretty good privacy. It is a widely used encryption program that provide secure communication for email messages. It uses a combination of symmetric key and public key cryptosystem to ensure confidentiality, integrity and authenticity of email communication.

Working of PGP in email security

Encryption

PGP uses symmetric key encryption to encrypt the actual content of email message. A unique session key is used to encrypt the message. This ensures that only the intendent recepient could decrypt and read the email message.

Public key encryption

PGP uses public key encryption to securely exchange session key used for symmetric encryption. The sender encrypts the session key with the receiver's public key, ensuring that the recepient with the corresponding private key can decrypt the session key.

Digital Signature

PGP allow users to digitally sign their email message to ensure integrity and authenticity. The recepient can verify the signature of sender's by using sender's public key and make sure that the message has not been tampered and has been originated from sender.

Key management

PGP includes mechanisms for managing public keys, including key distribution, key revocation and key certification. Users can share their public keys with others by key servers or personally exchanging them. Key revocation allows users to invalidate compromised or outdated keys.

Web of Trust

PGP relies on decentralized trust model called web of trust. It is a system where individual personally validate the authenticity of public keys, creating a network of trust relationship to ensure reliability of encrypted communication.

2) S/MIME

S/MIME stands for secure multipurpose internet mail extensions. It is widely used email message security protocol that provides encryption, digital signing and authentication for email messages. It enhances the security of email communication by adding cryptographic attachments.

Key points of S/MIME

Encryption

It uses public key cryptography to encrypt the email message and ensure that only the intended recepient could decrypt the message.

and read it. It protects the confidentiality of sensitive information during transmission

Digital Signing
It allows users to digitally sign the email message using the private key. The digital signature provides integrity and authenticity to the message, ensuring that the message has not been tampered and originated from claimed sender. Recipient can verify by using sender's public key

Certificate Based System
It relies on digital certificates issued by trusted certification authority (CA). These certification binds user identity to their public key.

Interoperability
It is supported by major email client ∴ ensures interoperability

End-to-End Security
It provides end to end encryption preventing unauthorized access to email content

It is used to enhance the security and privacy of email communication, particularly for sensitive information and business communication