UNIT II

E-MAIL SECURITY & FIREWALLS

S/MIME

- Provides a secure way to send and receive MIME data
- Provides the following cryptographic security services for electronic messaging applications
  - Authentication
  - Message integrity
  - Non-repudiation of origin (using digital signatures)
  - Data confidentiality (using encryption)
  - Supplementary service - Message Compression

S/MIME

- Definitions
  - ASN.1 :
    - Abstract Syntax Notation One
  - BER:
    - Basic Encoding Rules
  - DER:
    - Distinguished Encoding Rules
  - Certificate:
    - Name to a public key with a digital signature
  - CRL:
    - The Certificate Revocation List
  - Attribute certificate:
    - Authorization information
  - Sending agent:
    - Software that creates S/MIME
  - Receiving agent:
    - Software that interprets and processes S/MIME CMS objects
  - S/MIME agent:
    - User software that is a receiving agent, a sending agent, or both.

S/MIME

- *CMS*
  - Cryptographically protected message
  - List options in content and algorithm support
    - **Digest Algorithm Identifier**
    - **Signature Algorithm Identifier**
    - **Key Encryption Algorithm Identifier**
  - Details regarding the use of the cryptographic algorithms
    - Support six different content types:
      - **Data**
      - **Signed data**
      - **Enveloped data**
      - **Signed-and-enveloped data**
      - **Digested data**
      - **Encrypted data**
    - There are two classes of content types
      - Base -Data with no cryptographic enhancement
      - Enhanced - cryptographic enhancements
        - » Encrypted
        - » Encapsulated -Outer content contains the inner enhanced content

S/MIME

- **Enhanced Security Services for S/MIME**
  - ***Triple wrapped message***
    - **Signed, encrypted and signed again**
      - » Inside signature provides
        - Content integrity, Non-repudiation
        - Signed attributes can be used for access control to the inner body
      - » The encrypted body provides
        - confidentiality
      - » The outside signature provides
        - Authentication, Integrity
        - These attributes can be used for access control and routing decisions

S/MIME

- *Security Services with Triple Wrapping*
  - **Receipt request -** must be requested for inside signature, not in the outside signature
  - A secure mailing list agent may **change the receipt policy**
  - A **security label attribute** may be included in either the inner signature or the outer signature, or both
    - The inner security label is used for access control decisions related to the original plaintext content
    - The outer security label is used for access control and routing decisions related to the encrypted message.
  - Secure mail list message processing :-
    - Data used to form the inner signature is not changed by agent but it changes the outer signature.
  - Attributes should be placed in the inner or outer SignedData message
    - Some attributes must be signed
    - Signing is optional for others
    - Some attributes must not be signed
  - Some security gateways sign messages that pass through them
    - If the message is of any type other than a SignedData
      - Gateway Wrapp messgae in a SignedData block and MIME headers and then sign
    - If the message is a SignedData
      - Gateway Can sign the message by inserting SignerInfo into the SignedData block

S/MIME

- *Signed Receipts*
  - **proof of delivery**
  - **Inform that recipient was able to verify the signature**
  - This receipt is **bound to the original message**
  - This service may be requested **only if a message is signed**
  - Receipt may be encrypted
  - Requested by the originator of the message and send by the message receiver
  - Receipts are requested only for **the innermost Signed Data layer**
  - Only one receipt can be requested