Mail
- Set of headers built
- Data stored in fields
- RFC 822
  - Defined basic set of fields to transmit mail
  - Easy to spoof
  - Text/ASCII
- MIME standard (Multi-Purpose Internet Mail Extension)
  - Included attachments
  - Binary file converted to encoded format
    - Could then be transferred
  - Security layer established (S-MIME)
- Functions
  - Enveloped Data
  - Signed Data
  - Clear Signed Data
  - Signed/Enveloped Data
- Problems
  - Requires clients know S-MIME
- DNS
  - Administrative domain level takes responsibility
  - ISP
  - One domain able to query another for information
- Components
  - Message User Agent (MUA)
  - Message Handling System
  - Message Transfer Agent
MUA (Client email)
- Peer to peer relationship
- Also needs to talk to transfer system
MTA, similar to routers
- Determines path needed to transfer mail
Message Submission Agent
- May need to specify protocols used
- MTA -> MSA -> MUA normally
DHIM allows transmission system with/without not at user-level
- Signed by administrative domain
- Can't have spoofed origination

SSL: Secure Socket Layer (similar to TLS)
- Two layer protocol
  - Record layer (bottom)
    - Initiates connection/session
    - Handshake protocol
      - Establishes session key
      - Establishes encryption/hash protocols
  - Higher level protocols
    - Handshake
    - Cipher Spec
      - Trigger use of for connection
    - Alert
      - Warning or Fatal (ends connection/error message)

Record level
- Provides confidentiality and integrity
SSL can be established at application layer or layer of session
TLS - Transport Layer Security

SLIDES

S/MIME provides the ability to sign and/or encrypt messages.

Base64 takes data and signature and converts it to readable ASCII / language format.

DKIM used by wide range of e-mail providers.

\[ \text{MUA} \rightarrow \text{MSA} \rightarrow \text{MTA} \rightarrow \text{MTA} \rightarrow \ldots \rightarrow \text{MUA} \rightarrow \text{MUA} \]

Message handling system (MHS)

\[ \text{MS} \]

\[ \text{MUA} \]

SSL / TLS widely used security service.
- Provided as part of protocol suite or embedded into specific packages.
- Set of protocols that rely on TCP.

Higher level protocols:
- Record Protocol → Fragments data, compresses and encrypts.
- IP

TLS Session: Association between client and server.
- Connection: Peer-to-Peer relationship.

Handshake Protocol:
- Establishes identity
- encryption and MAC algorithms
- Keys used