Electronic Mail - SMTP

- Asynchronous message delivery
  - delivers robustness and reliability

- Two types of agents:
  - User Agent (UA)
  - Message Transfer Agent (MTA)

- Two types of interactions (and protocols):
  - MTA to MTA
  - UA to MTA
MTA to MTA

- Simple Mail Transfer Protocol (SMTP)
  - covers single hop
  - no encryption
  - no authentication
  - there was supposed to be a “not so simple” mail transfer protocol
  - some problems were addressed by ESMTP (extended SMTP) and other procedural methods
UA to MTA

- UA and MTA on the same host (the old days)
  - UA and MTA communicate using files
  - use of host’s authentication methods

- UA and MTA communicate over a network (today)
  - SMTP was not designed for this
  - sending mail: SMPT with authentication
  - retrieving mail: POP-3 and IMAP (include authentication)
Electronic Mail - SMTP

- Asynchronous message delivery
  - delivers robustness and reliability

- Two types of agents:
  - User Agent (UA)
  - Message Transfer Agent (MTA)

- Two types of interactions (and protocols):
  - MTA to MTA
  - UA to MTA
MTA to MTA

- Simple Mail Transfer Protocol (SMTP)
  - covers single hop
  - no encryption
  - no authentication
  - there was supposed to be a “not so simple” mail transfer protocol
  - some problems were addressed by ESMTP (extended SMTP) and other procedural methods
UA to MTA

- UA and MTA on the same host (the old days)
  - UA and MTA communicate using files
  - use of host’s authentication methods

- UA and MTA communicate over a network (today)
  - SMTP was not designed for this
  - sending mail: SMPT with authentication
  - retrieving mail: POP-3 and IMAP (include authentication)
SMTP Server Actions

- SMTP server is deciding whether to accept an email message for delivery
  - **Local**: recognized user of the organization that runs the server:
    - by IP address
    - authenticated
  - **Global**: everyone else

<table>
<thead>
<tr>
<th>From:</th>
<th>To:</th>
<th>Local</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td></td>
<td>Deliver</td>
<td>Deliver</td>
</tr>
<tr>
<td>Global</td>
<td></td>
<td>Deliver (with caution)</td>
<td>Deny (unless authenticated)</td>
</tr>
</tbody>
</table>
Problem: SMTP was designed to deliver limited length, English text

Solution: MIME (Multipurpose Internet Mail Extensions)
- make everything look like text
- package it and mark it with content type so it can be unpacked and rendered on the receiving end
Network Security
Security

- A broad problem, we will look at securing communication protocols

- Objectives:
  - confidentiality
  - authentication
  - message integrity
  - non-repudiation

*Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract...*
Encryption

- **M** - message, **C** - ciphertext (encrypted text)
- Encryption: \( E(M) \rightarrow C \)
- Decryption: \( D(C) \rightarrow M \)
Encryption Categories

Secret method: \( E( ) \) and \( D( ) \)

Public method, secret key: \( E_k( ) \) and \( D_k( ) \)

Public method, public and private keys: \( E_{pubk}( ) \) and \( D_{privk}( ) \)