Computer and Network Security

Computer & Information Sciences & Engineering
University Of Florida
Gainesville, Florida 32611-6120
nemo@cise.ufl.edu

Electronic Mail Security
(Pfleeger Ch. 9, KPS Ch. 13, 14, 15, 16)

1 Electronic Mail Basics

- RFC 821 SMTP
- RFC 822 Mail format
- X.400
- Mail User Agent (MUA)
- Mail Handler
- Created in benign environment

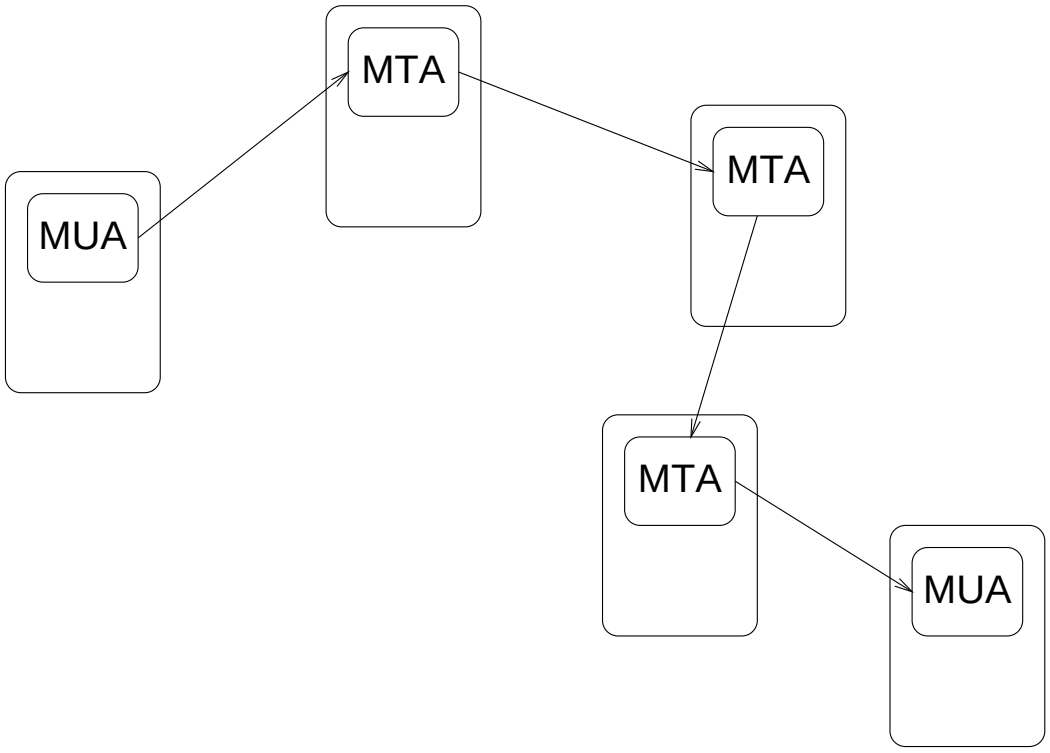

Figure 1:

1.1 RFC 821 SMTP

- 7-bit ASCII message character set
- adds log info to header - path info
- message text = header plus body

1.2 User Agent

- destinations derived from message header
- alias, mailing list, BCC processing

1.3 SMTP Sender

- initiates TCP connections to SMTP receivers at target hosts
- reduces destinations from destination list as sent
- optimizations (multiple recipients, multiple messages)
- handles retransmissions via TCP, not SMTP

1.4 SMTP Receiver

- awaits TCP connections from SMTP senders
- copies to mailbox(es) or to output queues (forwarding)
- handles transmission errors, disk space faults, etc.

2 MIME

Multipurpose Internet Mail Extensions
RFC 2045 - RFC 2049

2.1 Need for MIME

- SMTP cannot transmit binary files
- SMTP cannot transmit national language character text
- SMTP servers may reject messages that are too large
- ASCII-EBCDIC translations not standard
- SMTP cannot handle X.400 nontextual data
- non-conformant SMTP implementations

2.2 MIME Header Fields

- MIME-version
- Content-Type
- Content-Transfer-Encoding
- Content-ID *
- Content-Description *

* optional

2.3 MIME Content Types/Subtypes

- Text/Plain
- Multipart
  - Mixed
  - Parallel
  - Alternative
  - Digest
- Message
  - rfc822
  - Partial
  - External-body
- Image
  - jpeg
  - gif
- Video/mpeg
- Audio/basic
- Application
  - PostScript
  - octet-stream

multipart MIME type include boundaries

2.4 MIME Transfer Encodings

- 7bit
- 8bit
- binary
- quoted-printable
- base64
- x-token

3 Secure Email

3.1 Requirements

1. contents confidentiality
2. header confidentiality
3. contents integrity
4. header integrity
5. sender authentication
6. non-repudiation
7. certified delivery

3.2 PEM

1. use standard email without changes
2. X.509 certificates
3. always sign
4. may encrypt
5. base 64 encoding
6. multiple algorithms
7. algorithms specified in header encrypted with recipient's public key
8. duplicate headers
9. organizational email protection

3.3 PGP

1. web of trust
2. key ring
3. multiple algorithms
4. incompatible with PEM
5. individual user email protection