CprE 530

Lecture 17

Topics

- Email
  - SMTP
  - POP
  - IMAP
  - MIME

Email

Simple Mail Transfer Protocol:

First we will look at Electronic Mail systems in general and then we will look at SMTP. A basic electronic mail system performs four functions:

Creation: A user creates and edits a message, generally using a rudimentary editing capability. Most systems also allow the user to create a message using the system editor or a word processor, and then incorporate the resulting file as the body of the message.

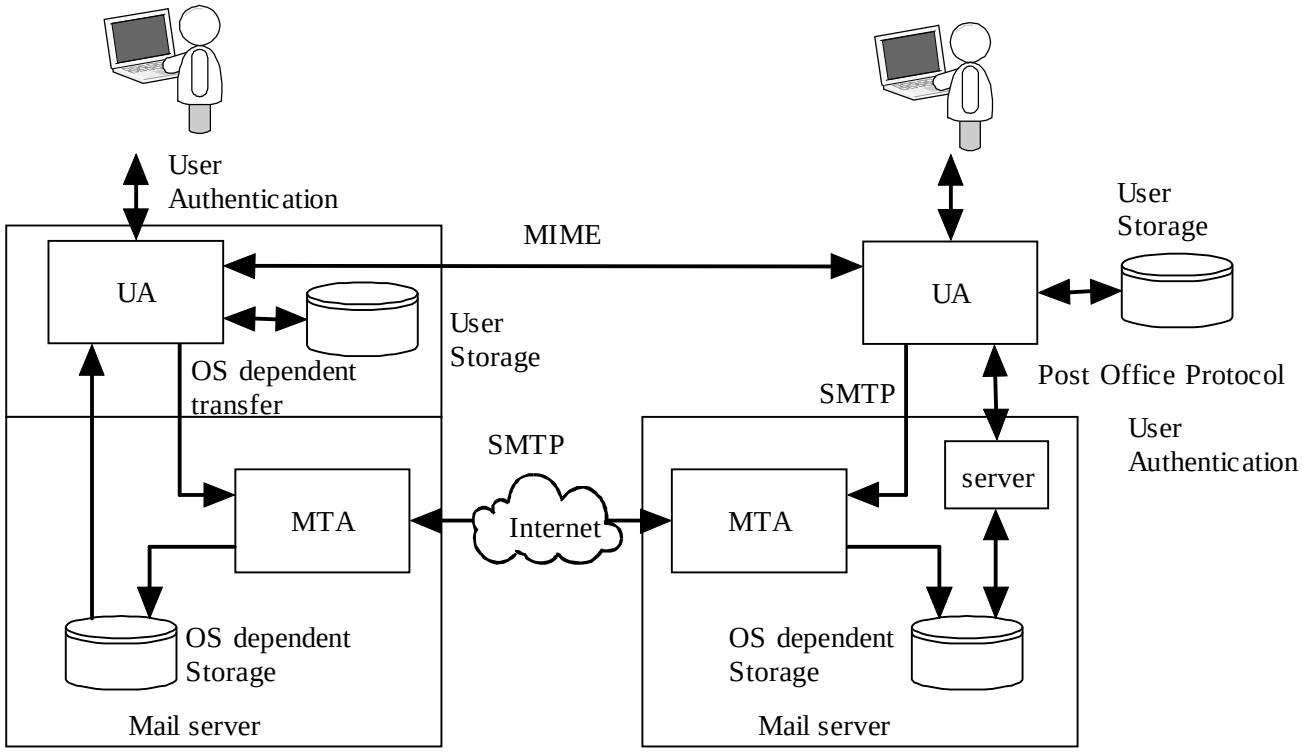
Email

Sending: The user designates the recipient (or recipients) of the message, and the facility stores the message in the appropriate mailbox(es)

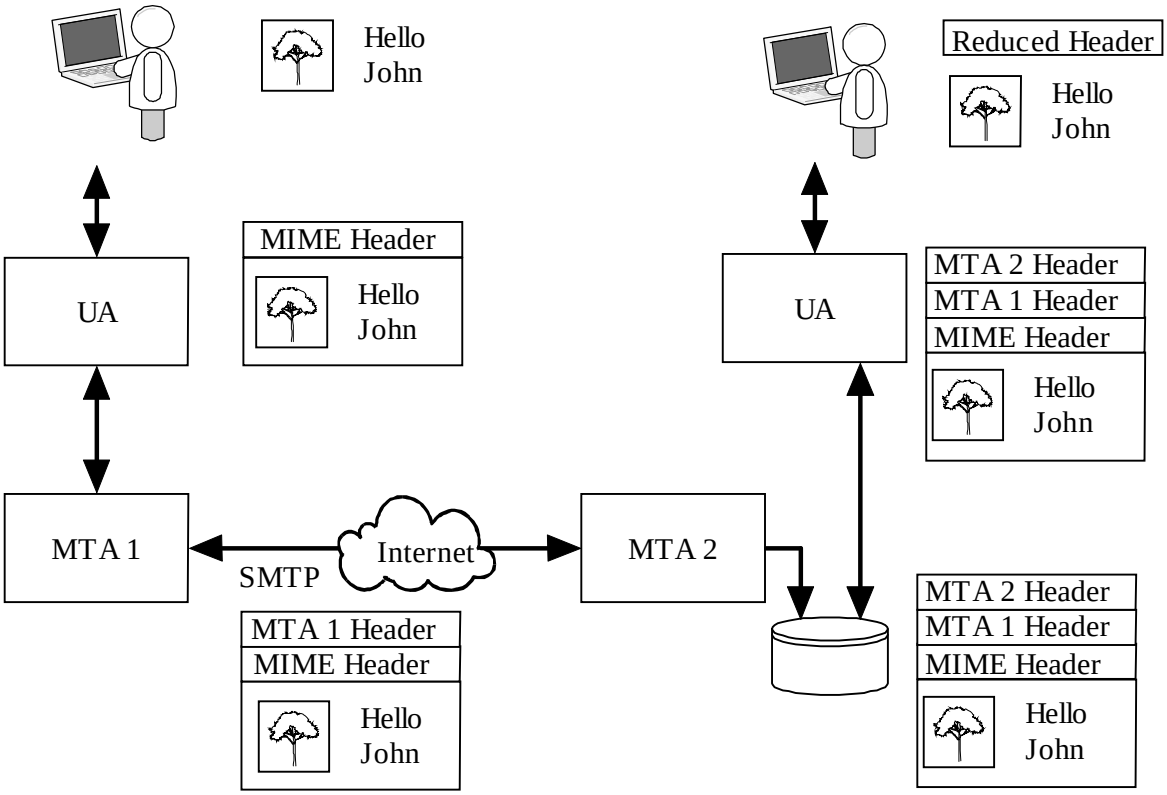
Reception: The intended recipient may invoke the electronic mail facility to access and read the delivered mail

Storage: Both sender and recipient may chose to save the message in a file for permanent storage

Email System



Email Message Format



Email

The SMTP protocol is the standard protocol for transferring mail between hosts. The protocol was defined in RFC 821 and later formalized as MIL-STD-1781.

SMTP is not concerned with the format or content of the messages themselves, with two minor exceptions.

SMTP requires a 7 bit ASCII character set.

SMTP adds logging information to message that indicates the path the message took.

Email

The SMTP protocol attempts to provide reliable operation, but does not guarantee to recover from hosts that lose files. No end-to-end acknowledgment is returned to a message's originator when a message is successfully delivered, and errors are not guaranteed to be returned either. However, the mail system is sufficiently reliable that this is not an issue.

In most cases mail goes directly from the mail originator's machine to the destination machine. However, mail will occasionally go through intermediate systems.

The SMTP protocol is made up of a set of simple commands.

Email

SMTP has 14 commands.

Command syntax is a set of 4 letter commands with parameters
Not all commands need to be implemented

The commands are:

CMD Syntax	Action
HELO <domain>	Used by the sending system to identify itself (HELO eeclass.ee.iastate.edu)

Email

CMD Syntax	Action
MAIL FROM: <path>	Identifies who the message is from. (MAIL FROM doug@iastate,edu) error messages have a NULL from field to prevent answers.
RCPT TO: <forward path>	Identifies who the message should be mailed to. There is separate RCPT for each recipient.

Email

CMD Syntax	Action
DATA	Indicates that the next transmission contains the message text. Terminated with a line containing <CR LF>.<CR LF>
RSET	Terminate current transaction
SEND FROM: <path>	Used instead of MAIL if message should be displayed on user's terminal.

Email

CMD Syntax	Action
SOML FROM: <path>	(Send or Mail) Used instead of MAIL if message should be mailed or displayed on user's terminal.
SAML FROM: <path>	(Send And Mail) Used instead of MAIL if message should be mailed and displayed on user's terminal.
VRFY <string>	Returns to the sender the full name of the user specified in the parameter
EXPN <string>	Returns to the sender a list of mailboxes corresponding to the alias provided

Email

CMD	Syntax	Action
NOOP		Performs no actions: returns a "250 OK" for debugging
QUIT		Sent after completion of transfer, prior to closing TCP connection.
TURN		Reverses the role of SMTP sender and receiver.

A reply code is returned for each command sent. The next slide shows the reply code format.

Email

The reply codes are designed to make implementation of SMTP easier. Each digit of the three digit code has a unique purpose.

First digit specifies whether the response was good, bad, or or incomplete.

The second digit specifies what type of error occurred.

The third digit details specific failures.

The values for the codes are given on the next slide.

Email

1XX Positive Preliminary Reply - The command has been accepted, but the receiver requires more information. (not used by SMTP, used by other protocols)

2XX Positive Completion Reply - The requested action has been successfully completed. A new request may be initiated.

3XX Positive Intermediate Reply - The command has been accepted, but action is being held, pending receipt of further information. The SMTP sender should send another command specifying this information.

Email

4XX Transient Negative Completion Reply - The command was not accepted, however, the error condition is temporary

5XX Permanent Negative Completion Reply - The command was not accepted.

Email

X0X Syntax Error or unimplemented commands

X1X Information: reply to requests for information

X2X Connections - reply to the request for connection

X3X Unspecified

X4X Unspecified

X5X Mail System - indicates the status of the receiver during, for example, a transfer.

The next slide has come common reply codes.

Email

211 System status or system help reply
214 help message
220 service ready
221 Service closing transmission channel
250 Requested mail action okay, completed
251 User not local; will forward to <forward path>
354 Start mail input
421 Service not available; closing channel
450 Mail box busy
451 requested action terminated; local error in processing
452 Requested action not taken; insufficient system storage

Email

500 Syntax Error, command unrecognized

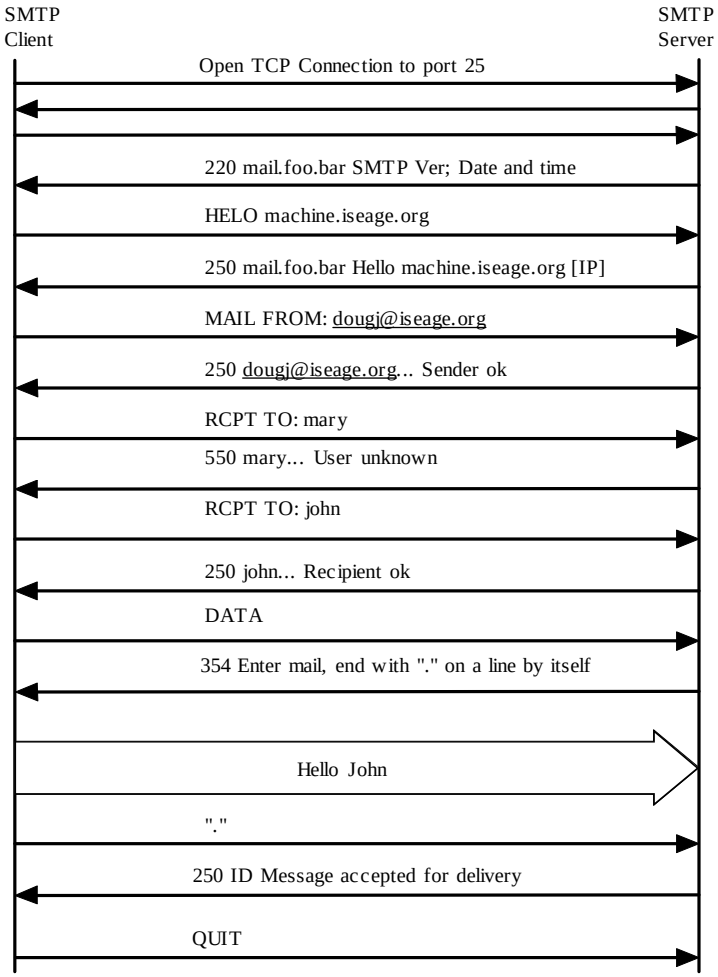
501 Syntax Error in parameters or arguments

502 Command not implemented

550 mailbox not found

551 user not local; please try <forward path>

554 transaction failed



SMTP

Header based

- Not common
- Some buffer overflow issues in old implementations

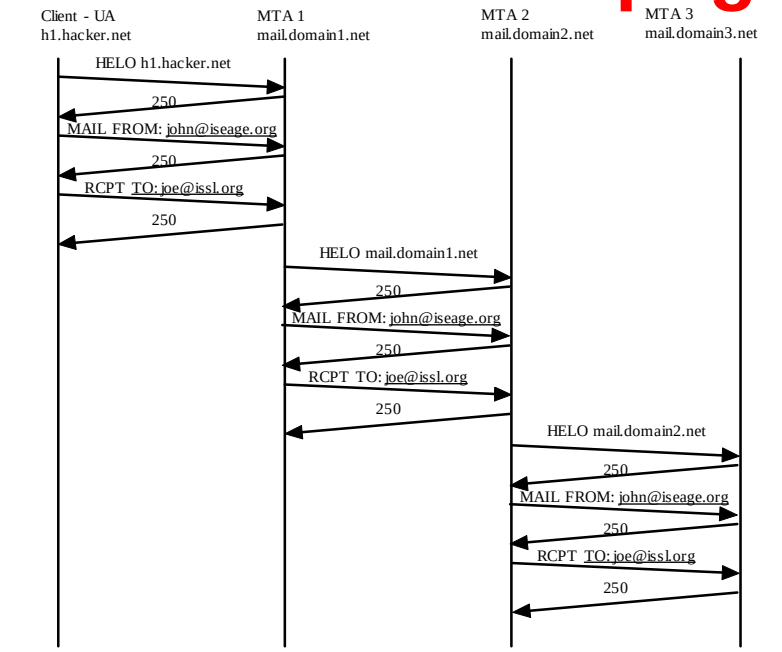
Protocol Based

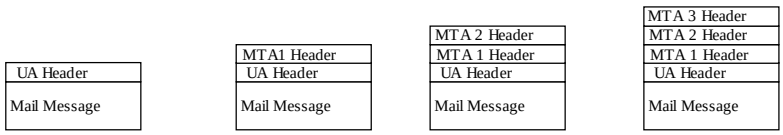
- Not common in command/response protocols
- Out of order commands are reported back as errors
- Multiple open connections could limit access to the email server.

Authentication Based

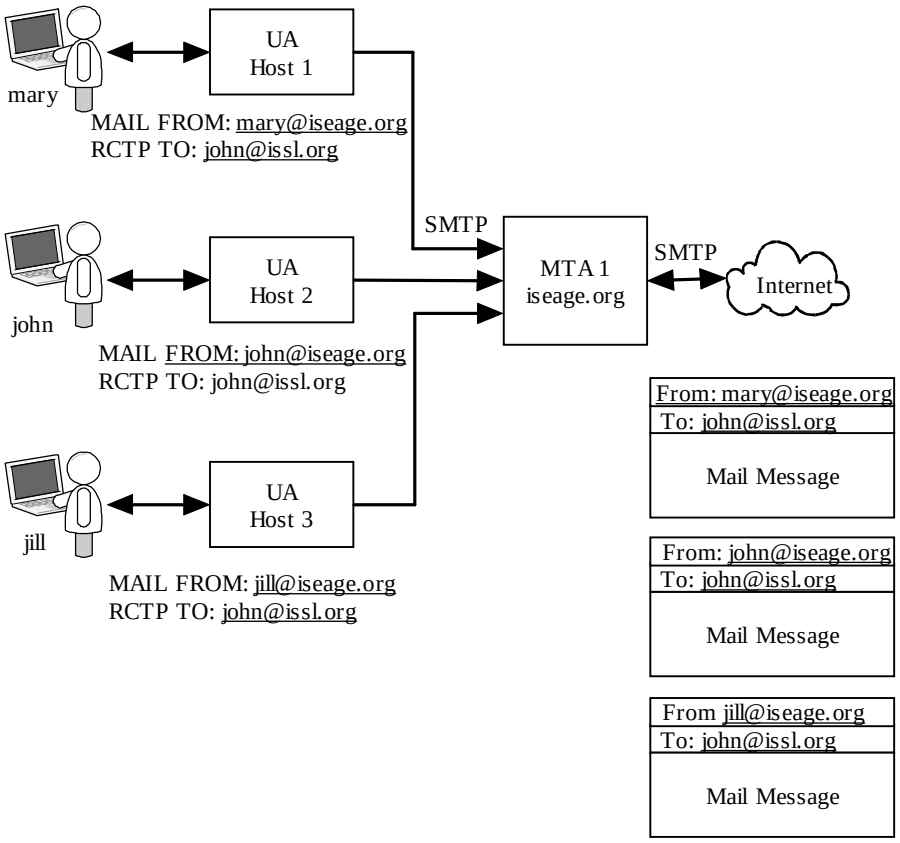
- Most common attack
- No authentication in SMTP
- Sender tells MTA the name of the sender
- Spam and phishing attacks
- Sometimes we want to spoof the senders address (email relay)

Email Address Propagation





Email Relay



Traffic Based

- Flooding of the email server
  - Too many messages
  - Messages are too large
  - Sending email to B from A with C as the return address could cause an attack on C
- Sniffing

General Countermeasures

- STARTTLS cause SMTP to use transport layer security (encrypted traffic)
- AUTH provides a method for users to authenticate with the MTA.
- Typically used for remote access to MTA for relaying
- Being discussed as a method to reduce spam