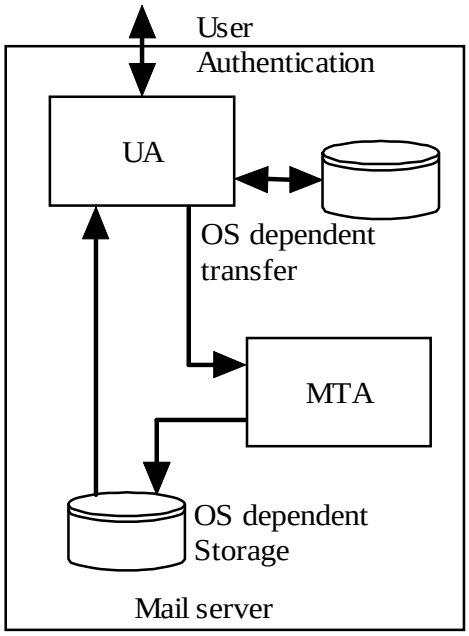
CprE 530

Lecture 18

Topics

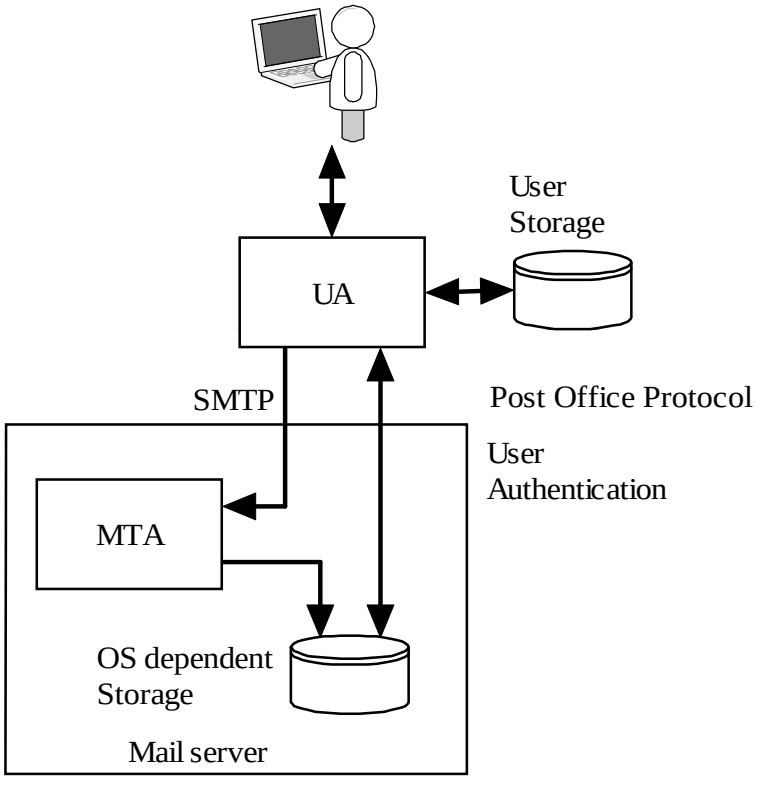
- Email
  - POP & IMAP
    - Protocol
    - Vulnerabilities and countermeasures
  - MIME
    - Vulnerabilities and countermeasures

Local User Agent



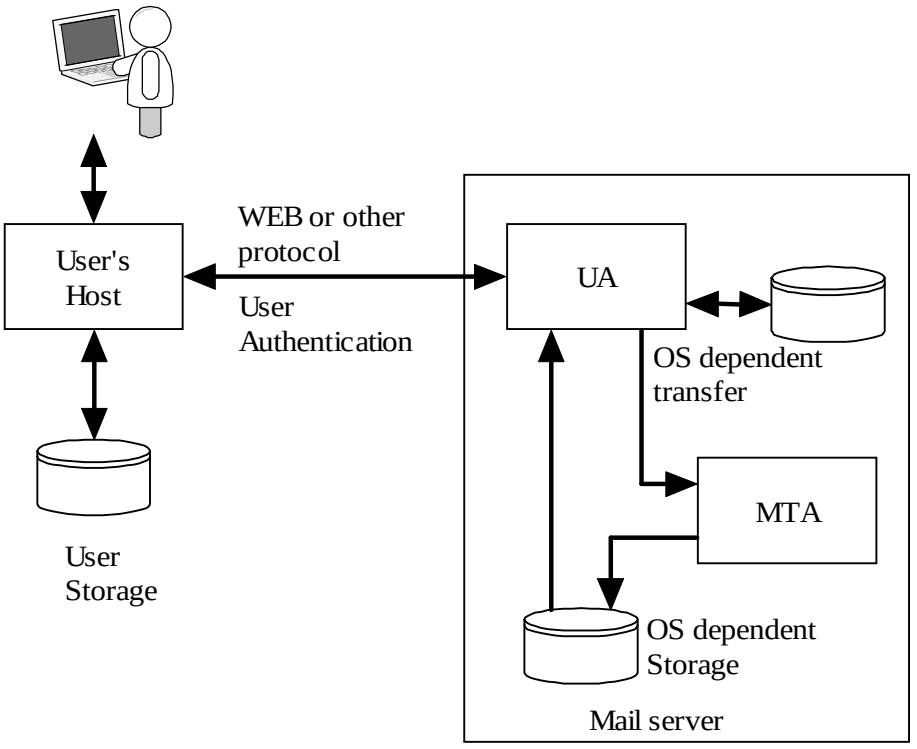
Local User agent

Remote User Agent



Remote User Agent

Remote access to local UA



Remote Access to Local User agent

POP

Post Office Protocol

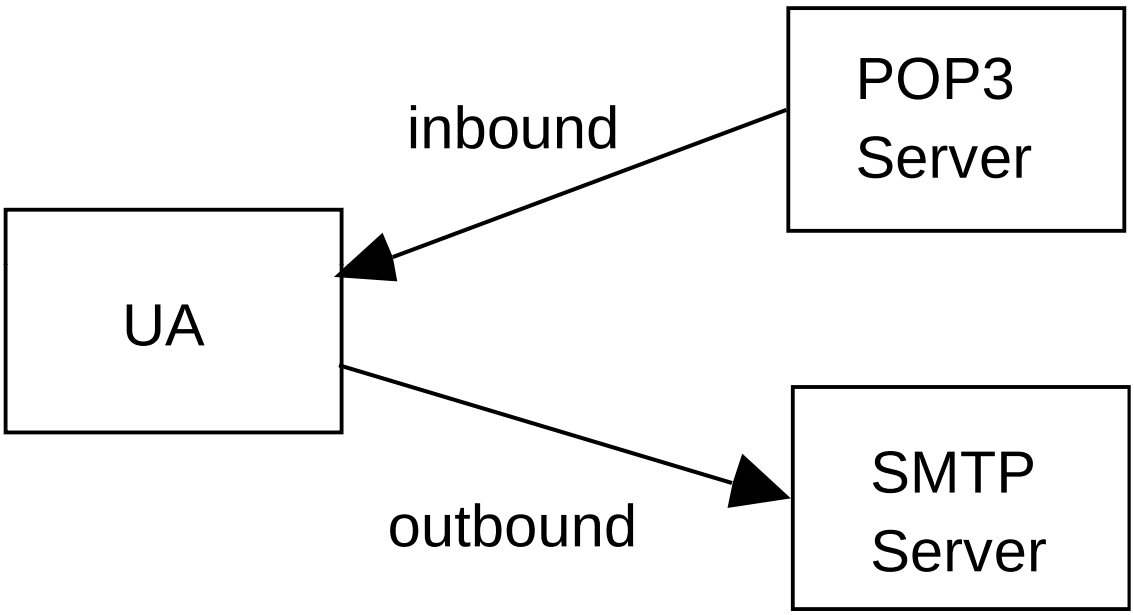
Used to transfer mail between the mail server and a PC

Provides user Authentication

POP3 protocol

- POP3 client “logs in” to a POP3 server (TCP port 110)
- Login name and password in clear text
- User can configure how often mail is checked
  - this means the login and password can be sent many times a day
  - easy to capture since when there is no mail there are only a few packets exchanged.

POP3 block diagram



POP3 Commands

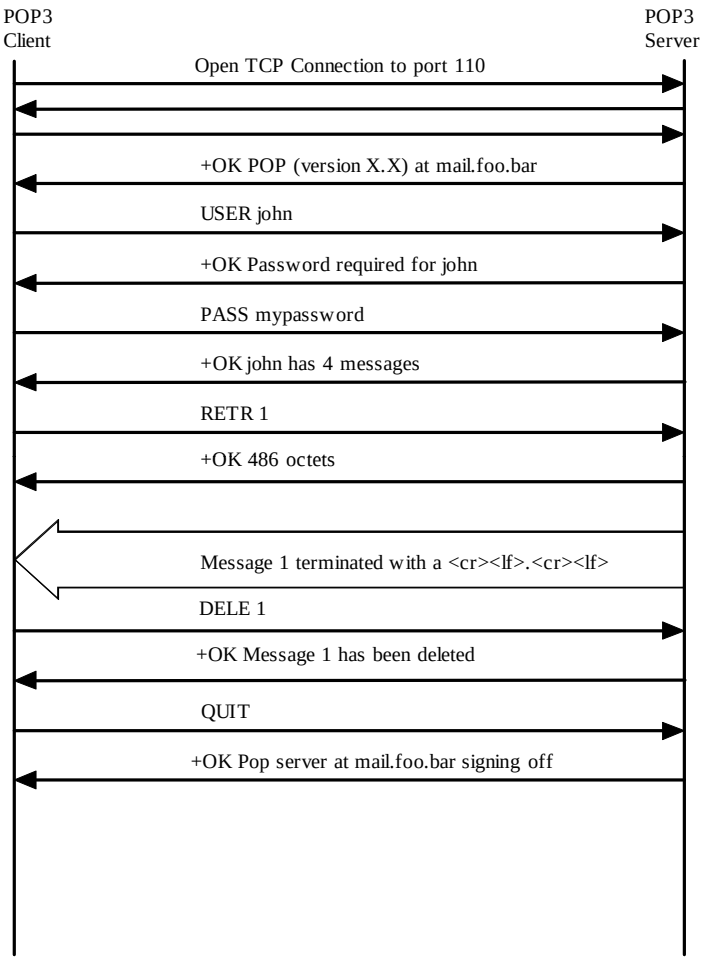
- USER name — Login name
- PASS string — User password
- STAT — returns number of messages
- LIST [msg] — returns the size of msg or all messages if [msg] is not supplied
- RETR msg — send client the full message [msg]
- DELE msg — Delete message from server
- NOOP — No operation
- RSET — Reset deletion indicators

POP3 Commands

- Quit — Quit the session
- APOP name digest — Optional authentication
- TOP msg n — return first n lines of message
- UIDL — returns a unique ID string for the requested message, does not change during session. Message ID can used to request message.

POP3 Responses

- Two response codes
  - -ERR message
  - +OK message

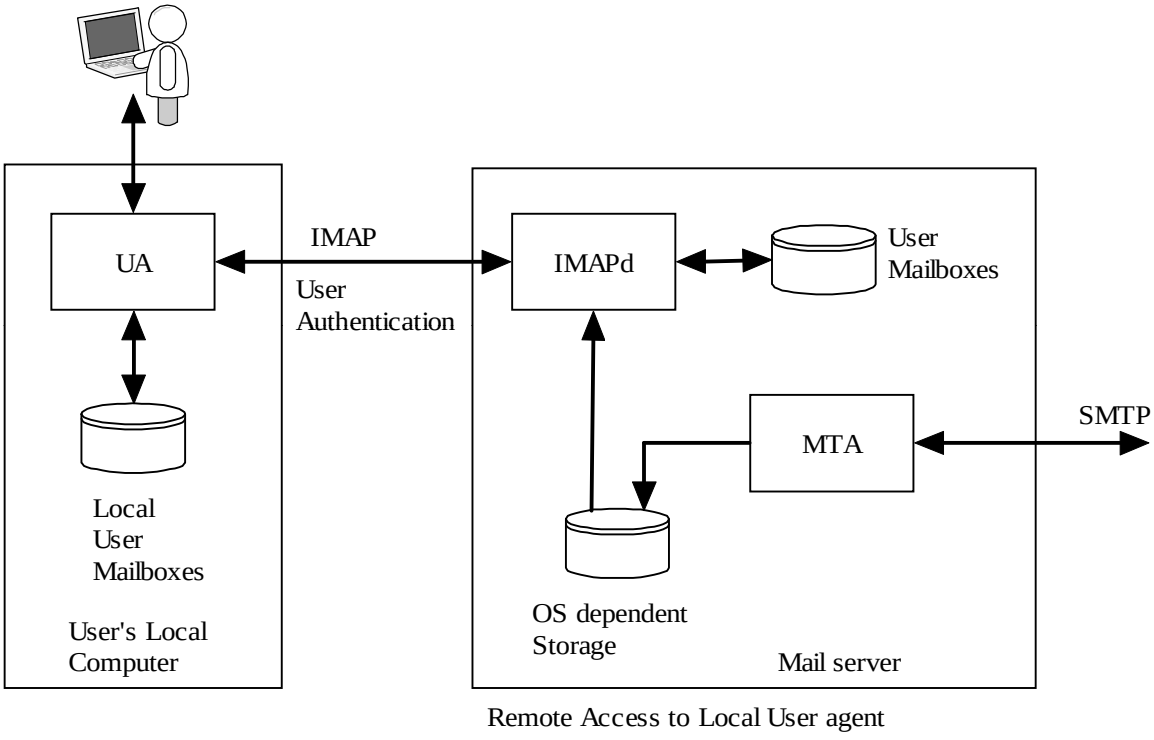


POP3 Protocol

IMAP

- Supports message retrieval
- Support message filing
- POP, does not work well in a multiple client configuration since mail is deleted after it is read.
- IMAP can keep messages on the server and an be used by multiple clients.

IMAP Mail Boxes



Remote Access to Local User agent

IMAP Commands

- CAPABILITY List server capabilities
- NOOP No operation
- LOGOUT
- AUTHENTICATE type
- LOGIN name passwd
- SELECT mailbox
- EXAMINE mailbox read only version of select
- CREATE mailbox
- DETELE mailbox

IMAP COMMANDS

- RENAME current-name new-name rename mailbox
- SUBCRIBE mailbox add mailbox to servers list of active mailboxes
- UNSUBSCRIBE mailbox
- LIST ref mailbox provide a list of mailboxes
- LSUB provide a list based on subscribe
- APPEND mailbox mess Append the message to the mailbox
- CHECK Flush mailboxes to disk
- CLOSE Close mailbox, all messages marked as deleted are removed

IMAP Commands

- EXPUNGE Remove messages marked as deleted
- SEARCH criteria Search the mailbox for messages that match
- FETCH message-set get message
- PARTIAL message len get partial message
- STORE
- COPY message-set Mailbox copy a message to another mailbox
- UID gets unique ID for messages

Header & Protocol based

- Very few header or protocol based attacks

Authentication Based

- User authentication over the network
- Password guessing using POP or IMAP
- Every attempt can be logged
- Restrict POP and IMAP authentication to know IP addresses
- Use web client for remote access

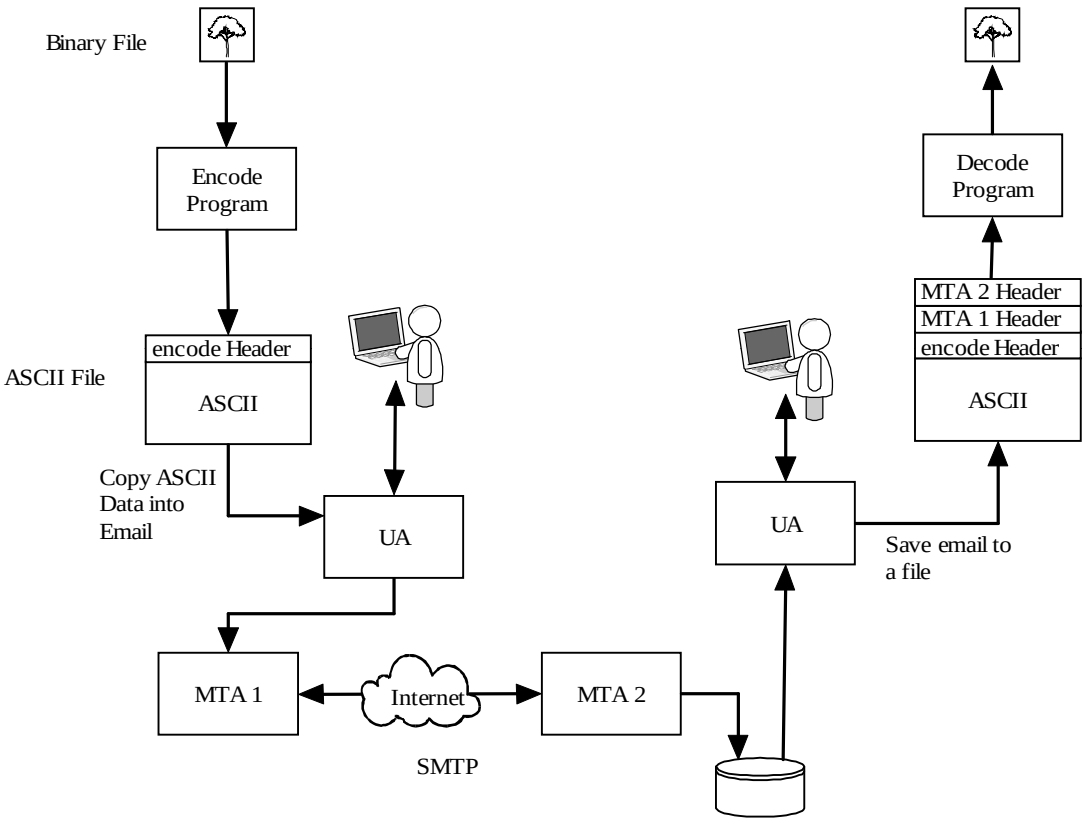
Traffic Based

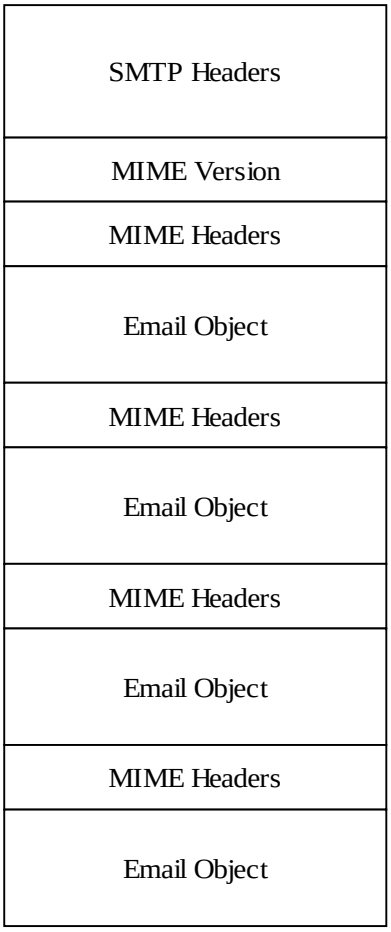
- Flooding is not much of an issue
- Sniffing is an issue
  - There are encrypted versions of both IMAP and POP, but they are not widely used.

MIME

- Multipurpose Internet Mail Extensions
- Email message format
  - Embedded pictures
  - Embedded code
  - Attachments

Encode and Decode





MIME Structure

MIME Headers

MIME Header	**Function**
MIME-Version:	Indicates a MIME message. The current version is 1.1
Content-Type:	Indicates the type of content contained in the message
Content-Transfer-Encoding:	Indicates how the content is encoded
Content-Id:	Optional Identifier used for multiple messages
Content-Description:	Optional description of the object that can be displayed by the user agent
Content-Disposition:	Optional description of the method to use to display the object in receiving the user agent

Content-Type

Type	Subtype	Description
	Plain	Unformatted text
Text	Html	Text in HTML format
Multipart	Mixed	Multiple ordered objects
	Parallel	Multiple object, not ordered
	Digest	Multiple ordered RFC822 objects
	Alternative	Alternate methods of representing the same object
Message	RFC822	Encapsulated message
	Partial	Part of a larger message
	External-Body	Object is a reference to an external message
Image	JPEG	JPEG Image
	GIF	GIF Image
Video	MPEG	MPEG movie
Audio	Basic	Audio object
Application	Postscript	Adobe Postscript object
	Octet-stream	8 bit binary object

Multipart MIME

- Next three slides show a multipart MIME message

```
Email Header
MIME-Version: 1.0
UA Header
Content-Type: multipart/mixed;
 boundary="------------090603080000040609050705"

This is a multi-part message in MIME format.
```

```
----------090603080000040609050705
Content-Type: multipart/alternative;
 boundary="------------000407030803000901080005"

  --------------000407030803000901080005
  Content-Type: text/plain; charset=ISO-8859-1;
  format=flowed
  Content-Transfer-Encoding: 7bit

  ASCII text message

  --------------000407030803000901080005

  Content-Type: multipart/related;
   boundary="------------080803090003030603090002"


  --------------080803090003030603090002
  Content-Type: text/html; charset=ISO-8859-1
  Content-Transfer-Encoding: 7bit

  HTML Text
   <img src="cid:part1.09040604.05020804@iastate.edu"
  alt=""><br>
  HTML Text

  --------------080803090003030603090002
  Content-Type: image/gif;
   name="logo.gif"
  Content-Transfer-Encoding: base64
  Content-ID: <part1.09040604.05020804@iastate.edu>
  Content-Disposition: inline;
   filename="logo.gif"

  GIF File in base64

  --------------080803090003030603090002--

  --------------000407030803000901080005--
```

OR

```
--------------090603080000040609050705
Content-Type: image/gif;
 name="logo.gif"
Content-Transfer-Encoding: base64
Content-Disposition: inline;
 filename="logo.gif"

GIF File in base64

--------------090603080000040609050705--
```

Content-Description
Content-Disposition

- Content-Description: <description>
  - Lets user “tell” the User Agent what type of file is attached
  - Allows malicious code to look like something else
- Content-Disposition: (Inline, Attachments)
  - Allows inline documents which will be displayed by the user agent
  - Allows malicious code be open automatically

Header based

- Headers can be used to hide actual content type
- HTML documents with hyperlinks where the text is different than the link
- Countermeasures:
  - User education

Protocol Based

- Different that normal protocols (no message exchange)
- Attachments can be malicious (viruses, worms, Trojan horses.
- Some can be auto opened (inline)
- Countermeasures:
  - Disable UA functions
  - Scanners, filters
  - Education

Authentication Based

- MIME does not support authentication
- Can support email monitoring
  - "Web Bugs"
    - 1x1 pixel picture stored on a web site
    - When email is read the file is downloaded
    - Web server will log access to the file and information about the machine that accessed it.
- Countermeasures:
  - Disable User Agent function to auto display pictures

Traffic Based

- Enables flooding of the email server
  - Large messages
- Sniffing