LinxChix

Email And Exim

Mail agents

- MUA = Mail User Agent
- Interacts directly with the end user
  Pine, MH, Elm, mutt, mail, Eudora, Marcel, Mailstrom, Mulberry, Pegasus, Simeon, Netscape, Outlook, ...
- Multiple MUAs on one system - end user choice

- MTA = Mail Transfer Agent
- Receives and delivers messages
  Sendmail, Smail, PP, MMDF, Charon, Exim, qmail, Postfix, ...
- One MTA per system - sysadmin choice

Message format (1)

```
From: Philip Hazel <ph10@cus.cam.ac.uk>
To: Julius Caesar <julius@ancient-rome.net>
Cc: Mark Anthony <MarkA@cleo.co.uk>
Subject: How Internet mail works

Julius,
  I'm going to be running a course on ...
```

- Format was originally defined by RFC 822 in 1982
- Now superseded by RFC 2822
- Message consists of
  Header lines
  A blank line
  Body lines

Message format (2)

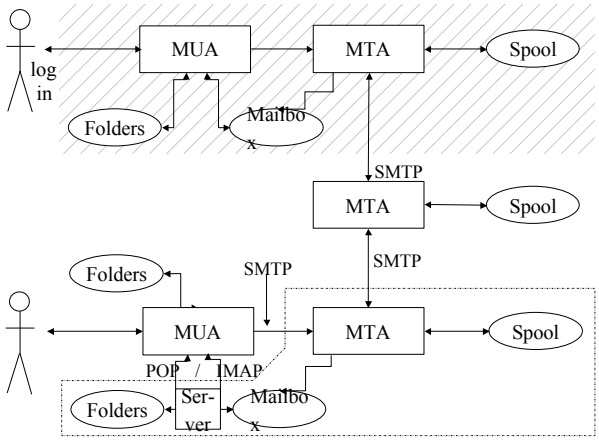
- An address consists of a *local part and a domain*
  `julius@ancient-rome.net`

- A basic message body is unstructured

- Other RFCs (MIME, 2045) add additional headers which define structure for the body

- MIME supports attachments of various kinds and in various encodings

- Creating/decoding attachments is the MUA's job



A message in transit (3)

- A message is transmitted with an *envelope:*
  `MAIL FROM:<ph10@cus.cam.ac.uk>`
  `RCPT TO:<julius@ancient-rome.net>`
- *The envelope is separate from the RFC 2822 message*
- *Envelope (RFC 2821) fields need not be the same as the header (RFC 2822) fields*
- *MTAs are (mainly) concerned with envelopes*
  Just like the Post Office...
- *Error ("bounce") messages have null senders*
  `MAIL FROM:<>`

An SMTP session (1)

```
telnet relay.ancient-rome.net 25
220 relay.ancient-rome.net ESMTP Exim ...
EHLO taurus.cus.cam.ac.uk
250-relay.ancient-rome.net ...
250-SIZE 10485760
250-PIPELINING
250 HELP
MAIL FROM:<ph10@cus.cam.ac.uk>
250 OK
RCPT TO:<julius@ancient-rome.net>
250 Accepted
DATA
354 Enter message, ending with "."
Received: from ...
     (continued on next slide)
```

An SMTP session (2)

```
From: ...
To: ...
etc...
.
250 OK id=10sPdr-00034H-00
quit
221 relay.ancient-rome.net closing conn...
```

SMTP return codes

- ***2xx OK***
- ***3xx send more data***
- ***4xx temporary failure***
- ***5xx permanent failure***

Email forgery

- It is trivial to forge unencrypted, unsigned mail
- This is an inevitable consequence when the sender and recipient hosts are independent
- It is less trivial to forge really well!
- Most SPAM usually contains some forged header lines
- Be alert for forgery when investigating

Use of the DNS for email (1)

- Two DNS record types are used for routing mail
- *Mail Exchange (MX) records map mail domains to host names, and provide a list of hosts with preferences:*

```
hermes.cam.ac.uk. MX 5 green.csi.cam.ac.uk.
                  MX 7 ppsw3.csi.cam.ac.uk.
                  MX 7 ppsw4.csi.cam.ac.uk.
```

- *Address (A) records map host names to IP addresses:*

```
green.csi.cam.ac.uk.  A  131.111.8.57
ppsw3.csi.cam.ac.uk.  A  131.111.8.38
ppsw4.csi.cam.ac.uk.  A  131.111.8.44
```

Use of the DNS for email (2)

- MX records were added to the DNS after its initial deployment
- Backwards compatibility rule:
  If no MX records found, look for an A record, and if found, treat as an MX with 0 preference
- MX records were invented for gateways to other mail systems, but are now heavily used for handling generic mail domains

Routing a message

- Process local addresses
  - Alias lists
  - Forwarding files
- Recognize special remote addresses
  - e.g. local client hosts
- Look up MX records for remote addresses
- If self in list, ignore all MX records with preferences greater than or equal to own preference
- For each MX record, get IP address(es)

Delivering a message

- Perform local delivery
- For each remote delivery
  Try to connect to each remote host until one succeeds
  If it accepts or permanently reject the message, that's it
- After temporary failures, try again at a later time
- Time out after deferring too many times
- Addresses are often sorted to avoid sending multiple copies

Relay control

- Incoming: From any host to specified domains
  e.g. incoming gateway or backup MTA
- Outgoing: From specified hosts to anywhere
  e.g. outgoing gateway on local network
- From authenticated hosts to anywhere
  e.g. travelling employee or ISP customer connected to remote network
- Encryption can be used for password protection during authentication
- Authentication can also be done using certificates