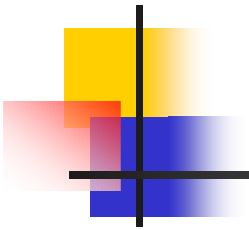
# “Spam, Scams and Filtering
## (and incontrovertible proof that most spammers are young males !)"

Les Hatton

CISM, Kingston University
L.Hatton@kingston.ac.uk

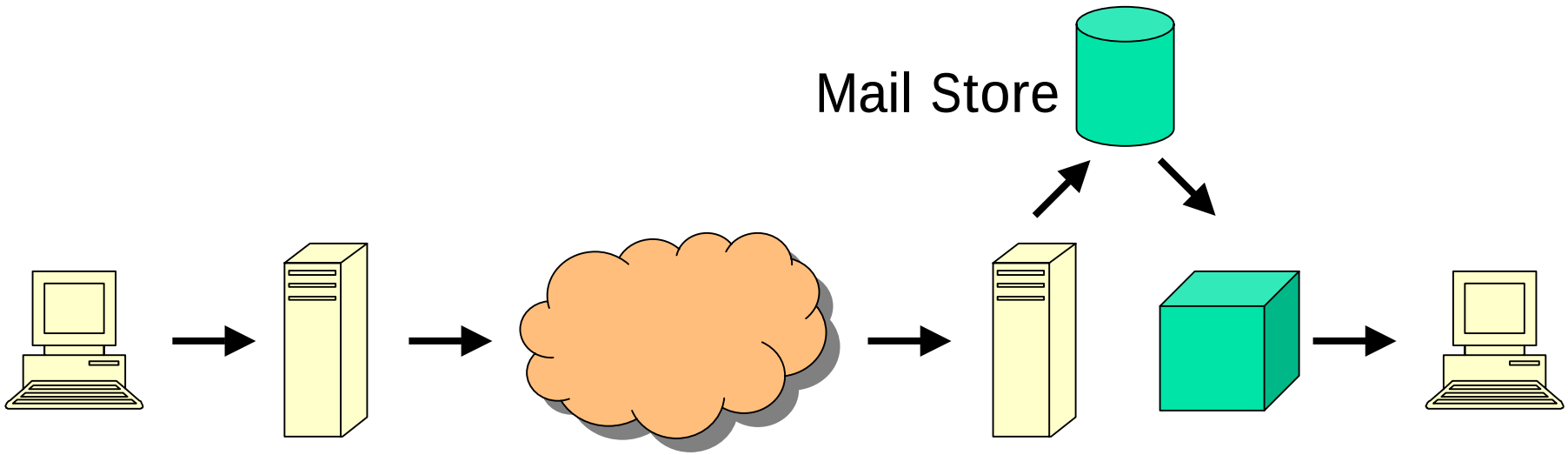
Version 1.2: 10/Dec/2008

# Overview



- Overview
  - The basics
  - The threat landscape
  - Commercial and non-commercial filtering
- Defence in Depth
- Wrap-up

# The basics: A ➔ B



# The basics: Headers and Content

Envelope

Content

**Connect** mail.receive.com (an MTA responds)

HELO mail.send.com (an MTA responds)

MAIL FROM: alice@send.com (an MTA responds)

RCPT TO: bob@receive.com (an MTA responds)

DATA (an MTA responds)

Date: ...

From: alice@send.com

To: bob@receive.com

Reply-To: ...

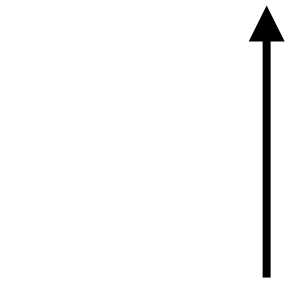
Message-ID: ...

Subject: ...

Blah blah blah

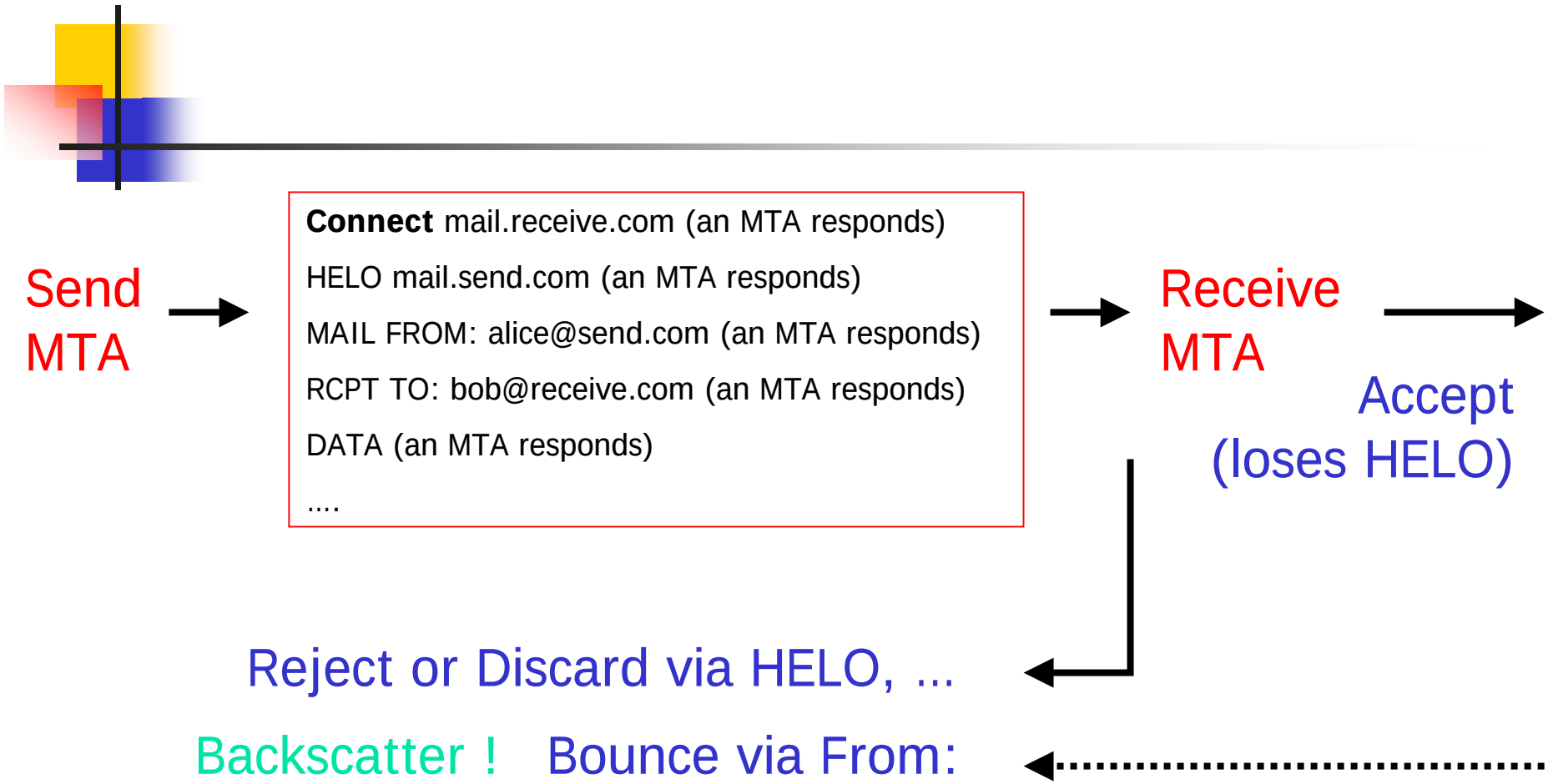
**Disconnect**

MTA



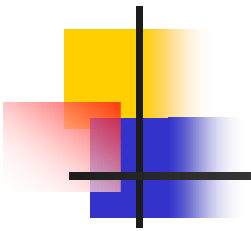
MUA

# The basics: Headers and Content



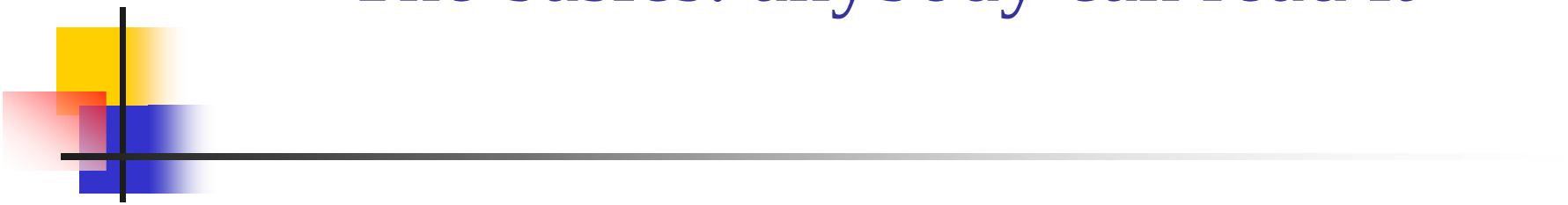

*** Reject as early as possible ***

# The basics: what can be forged ?



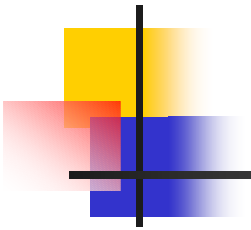
- Headers that can be forged
  - Subject, Date, Message-ID
  - Recipients: From, To, CC, BCC
  - Content body
  - Any arbitrary headers, X-Mailer …
  - All but the last Received header
- Headers that can ***not*** be forged
  - Last (top most) Received header
  - Originating mail server, specifically
    - IP address
    - Subsequent timestamps

# The basics: anybody can read it



- Nearly all e-mail is sent in clear as if you had written it on a postcard and asked a complete stranger to post it for you.
- It can be arbitrarily spoofed

# The threat landscape – e-mail borne toxins



- Spam
  - Density
  - Works of Art
  - Harvesting
- Scams
- Intrusions

# The threat landscape - spam

- For a single mail-server handling mail for 8 domains in 2-9 November

| | | |
|---|---|---|
| Total received | 836,106 | 100.00% |
| Discarded | 217,275 | 25.99% |
| Rejected | 618,000 | 74.00% |
| Rejected by content filtering | 13 | 0.002% |
| Delivered to users | 818 | 0.098% |
| (Missed spam / lost mail) | (0/0) | 0.00/0.00% |

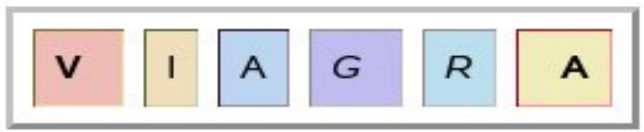
# The threat landscape – HTML works of art

```
<body>=09
<p>=09What's up?<a name=3D"#tprw"></a></p><a name=3D"#qpqr"></a><span name=3D"#twqp">=09</span><br><a
name=3D"#rtwp">  </a><table border=3D="6" cellspacing=3D"7" cellpadding=3D"1" width=3D"199">
<tr><td bordercolor=3D"#4B41CE" nowrap=3D"nowrap" valign=3D"baseline" bgcolor=
=3D"#D9F0BC"><strong>V</strong><font color=3D"#D9F0BC">b</font>  </td>
  <td nowrap=3D"nowrap" valign=3D"middle" bordercolor=3D"#69FA49" bgcolor==3D"#BCB6F0"
align=3D"center">   I </td><td bordercolor=3D"#67DA87" valign=3D"baseline" bgcolor=3D"#F0BCC3" align=
=3D"left" nowrap=3D"nowrap">   <b>A</b></td>
<td align=3D"center" bgcolor=3D"#F0C3BC" bordercolor=3D"
<td nowrap=3D"nowrap" bgcolor=3D"#D4F0BC" bordercolor=3D
color=3D"#D4F0BC">y</font>  </td>
<td align=3D"left" bordercolor=3D"#6852DC" valign=3D"top
<font color=3D"#F0B9BC">3</font>A=09</td></tr></table>
=09<br><strong></strong><table><tr><td>WWW</td><span>
</td><br><td>.</td><span name=3D"#rrtp"></span><td>COM</
</b><br><strong>=09</strong><p><span></span></p><span na
name=3D"#qqtp"></a></p>
</body>
```

**From:** "Riso Nuzzi" <cohered@nda.co.nz>
**To:** gundalf@oakcomp.co.uk
**Date:** 2008-08-07 00:10

**Spam Status:** Spamassassin

Heya,

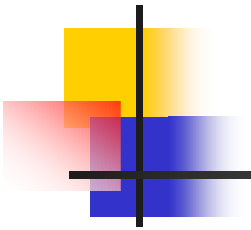



WWW . NEVOB . COM

# The threat landscape – harvesting e-mails

- “New virus coming – warn 25 of your friends …”
- “New speed camera – pass on to your friends”
- Assorted nonsense of a similar kind.

# The threat landscape – e-mail borne toxins



- Spam
- Scams
  - Nature
  - Density
- Intrusions

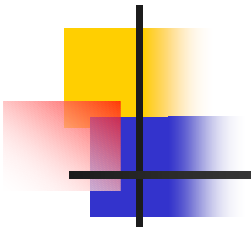
# The threat landscape – Nature of scams

- Of various kinds
  - Lottery (often the Netherlands)
  - “My left leg has been biten off by a mad cheetah and I have $4 million in da trouser leg” (Nigeria)
  - Phishing for account details
  - Pharming, DNS hijacking, …

# The threat landscape – Density of scams

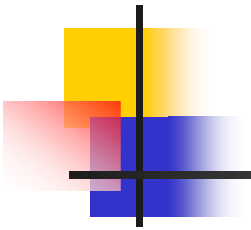
- Typical density
  - Approximately 2 per day per domain name but growing

# The threat landscape – e-mail borne toxins



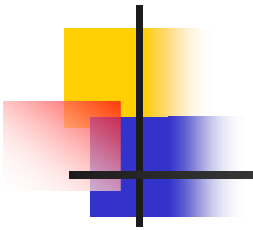
- Spam
- Scams
- Intrusions
  - Click-throughs
  - Attached files

# The threat landscape – Intrusions



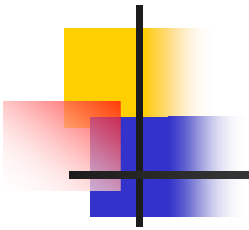
- Click-throughs:
  - Encourage clicking on a link to install a trojan or bot
- Attached files
  - Encourage clicking on a zip file with the subject, “Your invoice”, “Your receipt”, “Your …”

# Commercial and non-commercial filtering



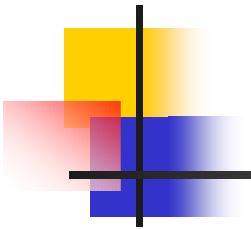
- Commercial
  - Buy tools
  - Buy service, (eg MessageLabs)
    - Your mileage may vary here. ML have missed an average of 15 a day in my mailbox since 6th September, mostly backscatter, with some days hopeless.
  - Use Google, yahoo or somebody
    - Be warned. All e-mail is read by tools for filtering. It would be easy to store keywords with other information already held on you.
- Non-commercial
  - Tools like SpamAssassin

# Overview



- Overview
- Defence in Depth
  - Layered protection and Postfix
- Wrap-up

# Layered protection and postfix - essentials



- Reject as early as possible in the transaction
- No open relays

**Connect** mail.receive.com (an MTA responds)

HELO mail.send.com

(an MTA responds ...)

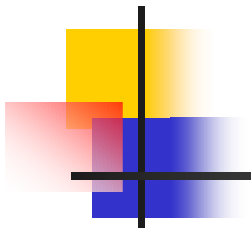
MAIL FROM: alice@totallybogus.com

250 Ok

RCPT TO: bob@notonyourserver.com

554 bob@notonyourserver.com Recipient address rejected: Relay access denied

# Layered protection and Postfix

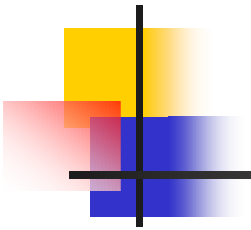


| | |
|---|---|
| smtpd_client_restrictions | **Server 220 smtp.receive.com ESMTP Postfix** |
| smtpd_helo_restrictions | Client: HELO mail.send.com<br>**Server 250 smtp.receive.com** |
| smtpd_sender_restrictions | Client: MAIL FROM: alice@send.com<br>**Server 250 OK** |
| smtpd_recipient_restrictions | Client: RCPT TO: bob@receive.com<br>**Server 250 OK** |
| smtpd_data_restrictions | Client: DATA<br>**Server 354 End data with <CR><LF>.** ... |
| header_checks | Client: To: bob@receive.com<br>From: alice@send.com<br>Subject: example |
| body_checks | Message body, blah blah, blah |
| external content filtering | Other content – Bayesian etc. |

# Layered protection and Postfix – typical installation with latest volumes

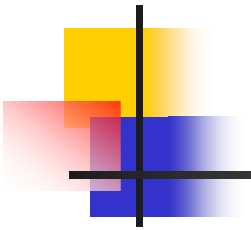
| | |
|---|---|
| smtpd_client_restrictions | **None** |
| (618,000) smtpd_helo_restrictions | reject self_helo, reject_non_fqdn_hostname, reject_invalid_hostname |
| (neg.) smtpd_sender_restrictions | reject_non_fqdn_sender, reject_unknown_sender_domain, blacklist |
| (216,000) smtpd_recipient_restrictions | Reject_non_fqdn_recipient, reject_unknown_sender/recipient_domain, reject_unauth_destination, reject unknown users, reject_rbl_client (spamcop etc.), **Greylist**, back scatter |
| (neg.) smtpd_data_restrictions | Reject_unauth_pipelining |
| (~ 200) header_checks | Different from/return-to, foreign character sets, various Windows skullduggery |
| (~ 200) body_checks | Other Windows skullduggery, tags, attachments, embedded .exe, ... |
| (~ 100) external content filtering | Viral filtering, sigs, creative html, SA, domain mismatch, embedded SURBL, cross-domain match |

# Layered protection and Postfix



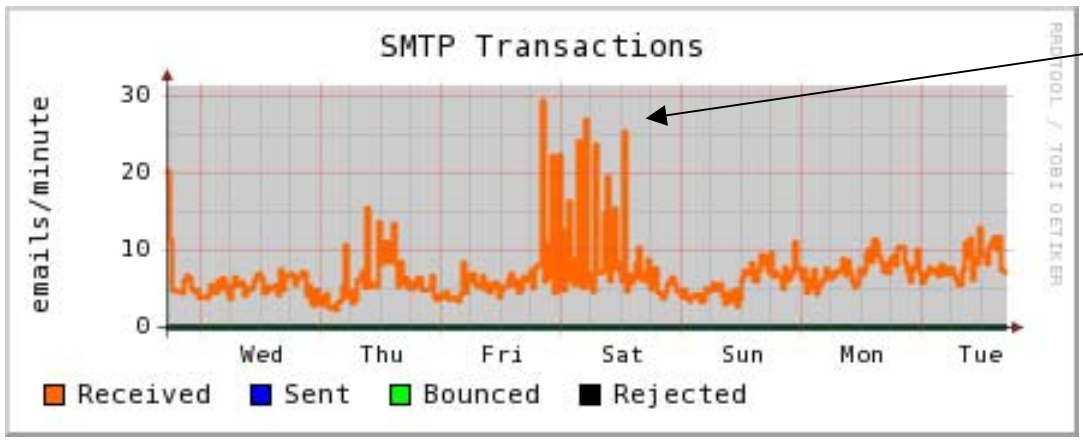
- About 75% of all e-mails can be rejected by being unable to say HELO properly.
- Implying that young mails [sic :-)] are responsible for most spam

# Miscellaneous



- Dealing with backscatter
- Unsubscribing
- Honeypots
- Whitelisting (as a last resort)

# Learning on the job

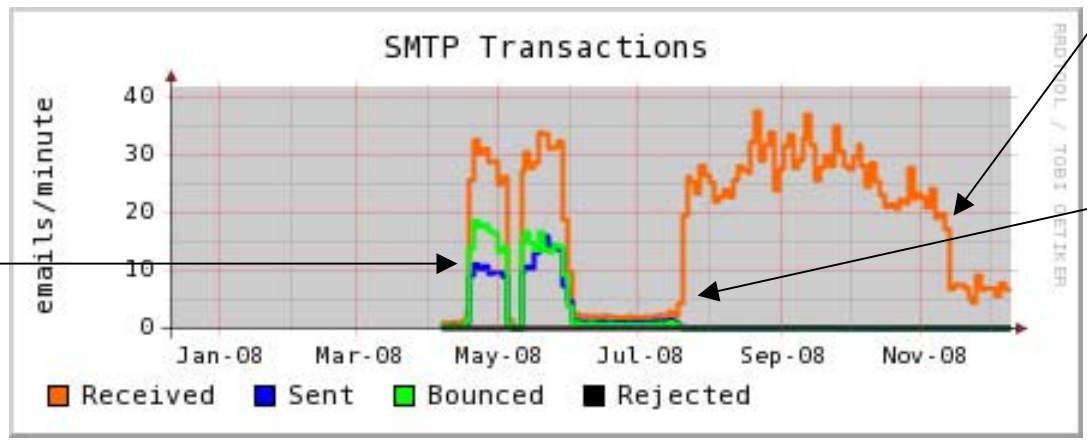



Weekend rubbish

Typical week

Attivo site closed in USA

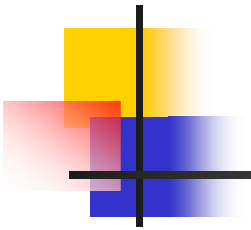
LH failing to understand the FormMail relay injection loophole




Silent discard, greylisting, RBL

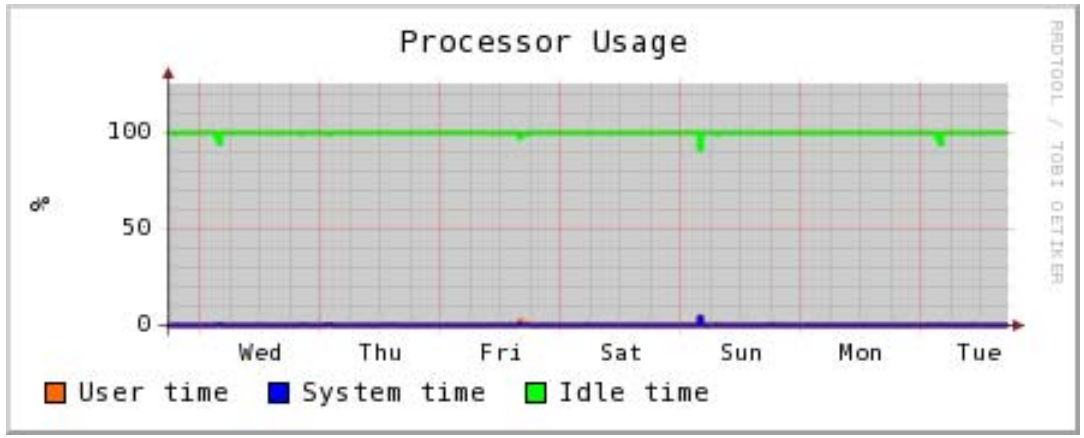
Year to date

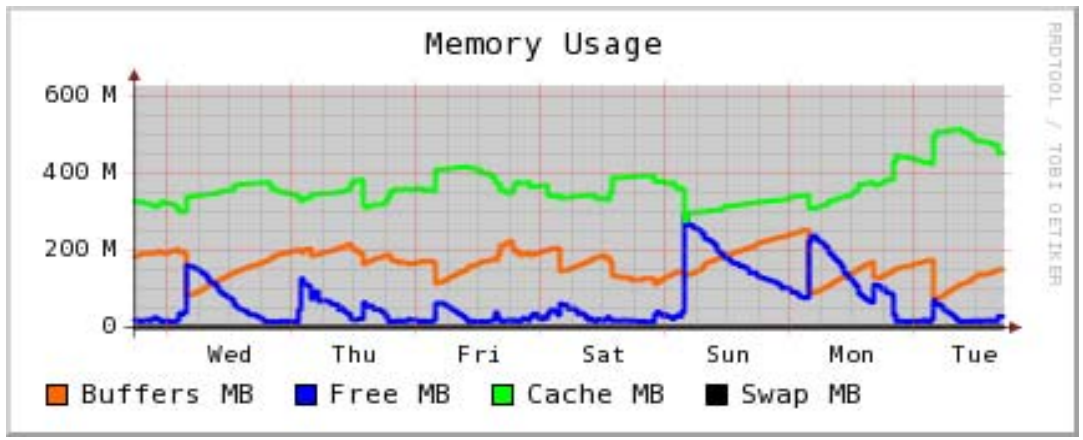
# Overview



- Overview
- Defence in Depth
- Wrap-up
  - Load on server
  - Threats in the pipeline
  - Things you need to know
  - Things still up our sleeve

# Load on server



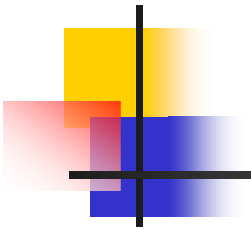
# Threats in the pipeline

- Scamming activity and identity theft is up and getting more sophisticated – be careful !
  - In 2007 3.6 million adults *claimed* to have lost US $3.2 billion.
  - In 2005, around GBP 24 million was lost in phishing.
- Spamming temporarily in a lull until Attivo servers allegedly move back to Russia
- Bot nets still growing sadly due to user ignorance and Windows vulnerability (~ 25% of all PCs)
- Pharming – DNS poisoning; watch your router.

# Threats in the pipeline: botnets

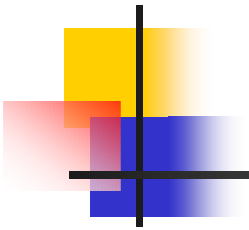
- Networks of PCs (20,000 – 500,000) controlled externally, often by IRC (Internet Relay Chat) servers.
- How they work
  - Botnet operator (herder) sends out viruses or worms infecting ordinary users' PCs.
  - The bot connects with the IRC server
  - Spammers purchase access to a botnet

# Things you need to know



- Perl :-)
- Postfix
- SMTP
- DNS
- TCP/IP

# Things still up our sleeve



- SPF
- Challenge / Response
- Lots of things we can do in content filtering

# Conclusions

- It is possible to operate as near to zero-spam as makes no difference
- Most spamming is still unsophisticated
- Scamming, (phishing, pharming) is getting much better and is a real danger rather than simply being a nuisance
- This will become more of a challenge

# References

**Loads of stuff on Wikipedia:-**

http://www.wikipedia.org/

**My writing site:-**

http://www.leshatton.org/