Anti-spam and anti-virus measures

DNS Blacklists

When mail arrives at our mailserver, our first line of defense is sendmail's mechanism to consult various DNS blacklists. These are lists maintained on the internet containing the IP addresses of know spammers. This mechanism is quite successful in stopping a large percentage of all unwanted mail (see statistics), but it cannot recognize spam when sent from a new, unknown source, so it cannot be the only defense. We have supplemented the DNSBL mechanism by some additional rules, like blocking mail where the sender address does not resolve to a valid internet address.

MailScanner

All mail, after passing the acceptence test, is processed through MailScanner, which is programmed to take the following actions:

1. Process mail through SpamAssassin for spam tagging;
2. Ordered List ItemProcess mail through the ClamAV and McAfee virusscanners;
3. Ordered List ItemQuarantine mail reported to be infected by a virus, or mail containing dangerous attachments or dangerous html.

Note: as of 18 November 2003, our MailScanner configuration ads a header with the short summary of the virusscan:

`X-LeidenUniv-MailScanner: Virusscan: Found to be infected`

for infected mails, or “Found to be clean” for uninfected mails.

Quarantine

If a virus or dangerous attachment is detected, you will receive a mail where the dangerous part has been stripped out and replaced by a virus warning like this one:

```
This is a message from the MailScanner E-Mail Virus Protection Service
```

```
The original e-mail attachment “eicar.com” was believed to be infected by a
virus and has been replaced by this warning message.
```