The "SPAM"

As is well known, mass mailing of unsolicited advertising messages ("junk mail" or "SPAM") is one of the most serious annoyances that users of electronic mail have to suffer on the Internet.

In an attempt to limit the impact of this pest, the University’s mail servers analyze all messages by various filters before delivering them. These filters try to detect and automatically mark the messages that they estimate can be "SPAM".

Other filters, also present on servers but not accessible to users, detect anomalous behavior of the sender servers and reject suspicious deliveries.

Anti-propaganda filters (SPAM) for UV users

Filter by content

The first of the anti-spam filters is a "content filter" (a filter that studies the content of messages). It is about "Spamassassin".

- What does Spamassassin do?

Spamassassin is a semi-intelligent filter that applies a whole series of rules - artificial intelligence - to decide whether or not a message is an unwanted message, with unsolicited propaganda.

- What does Spamassassin do?

If you decide that a message is a "spam", the spamassassin adds two headers ("X-Spam-Status:" and "X-Spam-Level:")) to the message. Example:

```
X-Spam-Status: LOW; 63
X-Spam-Level: xxxxxx +++
```

These headers are not normally visible to mail readers, but can be used in user-definable mail filters. The user can then decide what to do with the message.

The headers also contain a "score" (number of "x" in the text of "X-Spam-Level") that qualifies the message as spam with greater or lesser security as estimated by spamassassin.

On the other hand, for the qualification as "spam" to be clearly visible by the user, spamassassin modifies the "subject" of the message, putting it at the beginning the label "[SPAM?]".

- Do not use the "[SPAM?]" Of the subject as an object of the filters, as it may confuse them.

- Is Spamassassin effective?

The filter is not 100% efficient, and had a high percentage of hits (2003) when it was installed. Currently, its effectiveness has fallen dramatically because spammers have "adapted" their messages to make it very difficult to detect them with this type of filter. Even so, the filter is effective (currently around 30% correct - June 2005) and gives very few "false positives" (it is extremely rare for it to qualify as spam a message that is not). It continues to detect spam messages that are not detected by the other filters, so it is still advisable to have it activated.

- Why does spamassassin rate this message as "spam"?

You can ask Spamassassin to analyze a specific message and explain (in English) your reasons.

The form requests the text of the complete message with all the headers. For it, the simplest thing is to use Postman. Open the message and click on the dump icon (a red down arrow that appears in the "date" header). "Cut and paste" in its entirety the text obtained inside the form of the tester and press "check!".

Blacklist filter (RBL)

There are Internet lists that register computers that have been used very recently to generate spam. Other registers computers that have the mail service misconfigured and are very susceptible to being exploited by spammers.
These "blacklists" are maintained by a multitude of entities, even some of which are paid, and are commonly used by the vast majority of mail servers to qualify as "probable spam" all that is issued by the computers present in the lists.

- What does the filter do by blacklist?

The filter by blacklist finds, looking in the headers of the messages, who is the computer that has issued the message. If this computer is registered in any of the blacklists (currently four of them) that it consults, it marks it as "possible spam" adding an "X-RBL-Warning" header for each one of the blacklists in which it is found. message.

In the added header it is indicated which list is the one that has produced the warning and the computer (its IP number) suspicious. Example:

```
X-RBL-Warning: Warning: (211.240.40.237) listed as open relay by
abl-xbl.spamhaus.org - checked with rbl-milter
```

- Is the blacklist filter effective?

The blacklist filter is extremely effective. Filters currently (June 2005) of the order of 90% or more of the spam we receive.

- A friend sent me a message and it has been filtered by RBL ...

Tell your correspondent immediately, indicating which black list (indicated in the header X-RBL-Warning) is your server. Your mail administrators should take the immediate steps necessary to ensure that they will not issue (even accidentally, by infection, etc ...) more unwanted advertising and then use the blacklist forms to unsubscribe from it (or wait a few days to be automatically removed).

**Activation of the filtering**

The user can decide to redirect spam messages to a mailbox other than the one in which they were sent (for later review), or simply discard them. To do this, just define some mail filters on the server using the usual mechanisms for it: Email Filters.

Observe that you should never decide to "reject" spam messages, as the usual (99% of cases) is that the return address is false (non-existent address or someone who has nothing to do) and all that is achieved is saturate even more the servers and, what is worse, bother innocent people.

To facilitate the task of defining anti-spam filters, two buttons have been added to the filter definition form, one to automatically create the filter by content and another to automatically create the filter by blacklist.

- Steps to activate the filter by content
  - Enter email with username and password.
  - Press 'Settings'
  - Press 'Filters' in the 'Mail' section
  - In 'Create predefined Anti-Spam filter:' click on "By content"
  - That will make those messages qualified with at least one level of SPAM 4 (xxxx) go to a server mailbox called SPAM. This mailbox is accessible as a remote mailbox from the Postman or any other mail client program (IMAP).
  - In case our confidence in Spamassassin is very high, we can eliminate the messages instead of depositing them in that mailbox. This is done by selecting the "antispm" filter, pressing 'Modify' and selecting 'Delete' instead of 'Move messages to'.
  - Press 'Save'.
- Steps to activate the filter by blacklist
  - To activate the filter by blacklist, follow exactly the same steps as for the filter by content, but by clicking on 'Create predefined Anti-Spam filter' press "By blacklist".
  - To modify it, modify "antispm_rbl".

**Filters on the server**

Other filters against spam are configured on the server itself and can not be activated / deactivated at the user's will. The most important are:

- Filter by gray lists

**Note: The filter by gray lists has been deactivated in February 2014, since it is no longer effective.**

This filter is the one that can most affect users, after the filters by content and blacklists.

The filter by gray lists systematically rejects all the messages that arrive to it and only admits them when, after a certain time (5 min.), The sending server retries it with the same sender and recipient.

Every server that complies with the standards must retry, but most spam programs and viruses do not (yet). This allows discarding the servers "spammers" and reject their messages. This system has proven to be extremely effective.
The filter by gray lists allows today (January 2008) to discard almost 70-80% of spam messages.

But the filter by gray lists causes a delay of the mails. The delay depends on the time it takes the sending server to perform the retries. Typically you can wait for 15 to 30 minutes, but the delay can be several hours. Except in some cases of incorrect or unusual configuration of the sender's servers, the filter by gray lists DOES NOT cause loss of mail.

The gray list filter maintains an automatic white list, so that it does not delay messages at all when you already know that the sender-recipient pair is valid. Remember these pairs for more than a month, so users should not notice delays when communicating with regular correspondents.

The filter is also "unlocked" by gray lists when a sender from the university sends an external recipient. Successive answers will not be delayed.

**IP flow filter**

The flow filter stops attempts to deliver an excessive message flow to our servers. Deny access for several minutes to anyone who tries to send more than XX (ie 110) messages or make more than XX (ie 20) connections to the server in a period of 5 minutes. This filter only authorizes some known servers to exceed these limits. The daily statistics of the flow filter can be found in StatisticsCriba.

**Flow filter by sender**

The flow filter by sender blocks all senders who send more than **400 messages in 24 hours**. A sender is a user (the SMTP connection is authenticated) or the value of the "From:" header of the messages.

The filter is unlocked after 24 hours without any further attempt to send. Every new attempt extends the blockade 24 hours more!

If your mail is blocked by the flow filter by sender, make sure you have no active mail program that automatically retries pending shipments! In general, make sure you do not have pending shipments.

**Filter valid domains**

Only a few domains @ xxx.uv.es are registered as valid mail servers (domains) to receive messages. To install a new mail server, it is necessary to contact the SIUV to register it.

That is, if a user installs a PC with an SMTP server (very common in Linux), he should not expect to receive messages with him. In individual PCs it is assumed that mail clients will be used (Thunderbird, pine, Mail, Outlook, ...), not servers (Sendmail, Postfix, Exchange, ...).

**Other filters**

Apart from those mentioned above, other active filters against spam are:

- The "toloc" filter that prevents messages from non-existent users from entering our network.