EMBEDDED email server

The spam and extension filter identifies viruses and worms rejects (dangerous) attachments or renames them identifies spam e-mails and rejects them. How is it done?

Identification of viruses and worms

The most widespread and known viruses and worms are identified. E-mails with such viruses or worms are immediately deleted. The user is provided defense mechanisms against new viruses or worms in the new update.

Rejection / Renaming of (dangerous) attachments

The user has the option of deleting e-mails with particular attachments (e.g., .sys, .exe) or renaming their attachments into a non-executable extension (For this purpose, the last letter of the extension is replaced by a "-", e.g., ".exe" becomes ".ex-"). When the renamed attachments are saved onto the PC, they can be manually transformed back to their original state by the user.

Identification of spam (e-mails)

1. by filtering URL
Commercial spam (e-mails) are almost always sent in order to sell the receiver "something or other." Through such e-mails, the sender hopes to motivate the receiver to visit a certain Web page and buy a specific product. That is why spam (e-mails) always contain a link (URL) to a Web page where the advertised product can be purchased. These URL's are identified in the e-mail (it makes no difference if it is HTML or just text) and reduced to the domains (e.g.: If "http://www.superproduct.com/index/bestarticle/order.html" is found, then this chain of symbols is reduced to "superproduct.com"). Once found, such a chain of symbols is searched for in the **URL white List**. If it is found there, the e-mail is not spam. If the chain of symbols in not found in the **URL white List**, then it is searched for in the **URL black list**. If it is found there, the e-mail is spam and will be dealt with as such. It is also checked whether the e-mail address of the sender is among those in the white list of addresses. If the sender's address is found in the white list of addresses, then the e-mail is **not** considered spam, even if it has an URL entry which can be found in the URL black list.

2. by using the black list of addresses and white list of addresses
The black list of addresses contains e-mail addresses from which an e-mail should never be accepted. E-mails from e-mail addresses which have been entered into the white list of addresses are always accepted. The black list of addresses and white list of addresses have precedence over the URL black list and URL white list; the white list of addresses has the highest precedence. That means:

- if e-mail addresses are entered in the white list of addresses, then e-mails from these senders are always received, independent of whether they are also entered in the black lists.

- if e-mail addresses are entered in the black list of addresses, then the e-mails from these senders are always rejected, except when they are entered in the white list of addresses.

- e-mails which have URL entries listed in the URL black list are dealt with as spam, except when these URL's can be found in the URL white list or the e-mail has been entered into the white list of addresses.

Entries into both lists are performed manually.

3. by identifying so-called "dictionary attempts"
In this case, the spammer sends e-mails to a (very large) list of receivers of a target domain in which frequently occurring first and last names are used (e.g., john.smith@domain.com). This is done in the hope of coming across an actual e-mail address by chance. If an e-mail is addressed to more than three local receivers, the hit accuracy is analysed. If 75% of the receivers do not exist, then the e-mail is automatically marked as spam.

4. by using the NCT URL black list databank (updateable!)
If this function is configured, then the NCT URL black list databank is automatically downloaded from the NCT Web-server. For this purpose, it will be checked every four hours if a new version of the NCT URL black list databank is available. In this process, missing entries are added to the local URL black list from the NCT URL black list.
URL's of the NCT URL black list databank which can be found in the user's URL white list are not added to the user's local URL black list!

5. by using the "spam block account" option
If the "spam block account" option is set for a user's account, then all the e-mails which are sent to the user are dealt with as spam. This function can be used as follows:

a) If a received e-mail is classified as spam by the user, it can be sent on to a spam block account. This e-mail will be dealt with as spam in further processing. That means that the URL's in this e-mail are automatically entered into the local URL black list.

b) The "honey pot method"
A user's account with the "spam block account" option is used to cancel his/her registration at a spammer's site. Since the option of "canceling registration" (e.g., "Would you like to continue to receive e-mails yes/no") which many spammers offer is normally abused in order to determine whether an e-mail address is active, one actually attracts more spam from such spammers after the "cancellation." When "canceling" a user's account with the "spam block account" option at a spammer's site, the spammer sends spam to the spam block account. E-mails which are "attracted" in this way are immediately identified as spam and the URL's in this e-mail are automatically entered into the URL black list. This secures that all other users will not receive this spam.
(A further possibility of directing spam to the "honey pot" is to use the "spam block account" e-mail address in Newsnet now and again!)

6. through the setting: "Simplified Chinese" is spam (configurable)
The device can be configured so that an e-mail which consists of "Simplified Chinese", "BIG5" or "CSBIG5" symbols is automatically considered spam. In this way, often up to 10% of all potential spam e-mails are identified and dealt with accordingly.