

O Internet, how do you bug me? Let me tell you the ways  
A White Paper

Ben Corby  
Technical Director  
New Millennium Solutions Pty Limited  
8 July 2004

Many articles will tell you that electronic mail is being destroyed by unsolicited mail. Why? Because users receive not only unmanageable volumes of it, but mails that cause mischief to themselves and other Internet users. How have the volumes become unmanageable? There are many reasons, but the dominant one is that unwanted mail has become self-perpetuating.

Where does this mail come from? Are there people who should be in padded cells working long into the night sending unwanted mail to unwary recipients? Or, are they legitimate businesses simply trying to make a buck?

Any analysis of unwanted mail will show that most of the mail is not peddling products, but is a meaningless composition of names, domains and content. Most unwanted mail is mischievous rubbish.

What is worse, most unwanted mail is not only rubbish, it's now dangerous rubbish. Once unwanted mail was a nuisance; it had to be read and discarded. Then, a recipient had to be wary of unwanted mail as it might contain a virus that would render the recipient's computer unusable; now a recipient can get mail that will use the recipients' computer to send out more mail – and to the recipients address book, so the recipients friends are bugged as well!

How do the senders get the email addresses? Often by harvesting. This involves a server sending hundreds and sometimes thousands of messages to an email system with varied user names. Sooner or later, the combination will succeed. Harvesting can increase mail traffic to a server far beyond anything it has seen before. Harvest attacks are always random in timing and duration

There is a huge volume of unwanted mail and harvesting being passed from server to server, box-to-box, user-to-user, clogging commercial arteries with useless traffic.

You must choose one of two approaches when deciding a system to manage unwanted mail. The first is that you can read the mail, filter it according to its content and put suspect mail in a specific folder. The second is that you can challenge an unknown sender to identify him or herself; a process known as Challenge-Response. I am a firm believer in Challenge-Response. I think it's the best defense against unwanted mail.

The email server is the first line of defense against the volume of rubbish and against those who aim to maintain the volume. If that's the case, is there anything that a server can do to increase its defense? There certainly is and any worthwhile system will incorporate these techniques in its operation.

Challenge-Response provides some real advantages in network capacity management.

Once you have Challenge-Response, you can reject unwanted mail at the server. You can do this by using the SMTP protocol to refuse the message completely, thereby preventing over 90% of email traffic from even entering your network.

Most rubbish mail comes in waves and often from the same server. If the same server sends more than a certain number of messages to the same address in a given period, it is practical to stop challenging the messages and simply reject them.

Finally, if a server notices that there are multiple "rcpt to:" messages, as is the case in harvesting, then the server can slow down its response, thereby reducing the load on the server and the effectiveness of the harvesting.

All the above approaches are about reducing the load caused by unwanted mail and harvesting and about using network capacity effectively. It is no longer practical to increase network capacity to allow for unwanted email traffic; the traffic will increase in line with the capacity. It is now

necessary to stop the traffic and manage the load by other means. If people are seriously not using the Internet due to its frustrations and dangers, it's up to the designers and implementers to provide better mail management.

All trademarks are the property of their respective owners.  
Copyright New Millennium Solutions 2004.