

Challenge Response: Looking at the Real Benefits
A White Paper

Ben Corby
Technical Director
New Millennium Solutions Pty Limited
bcorby@new-ms.com
2 June 2004

How many articles do we read from how many people about how much they hate unsolicited email? Hundreds. I subscribe to a service that sends me details every day of the many articles written about unwanted email. I am now getting details of about 10 articles a day and most complain about the effect of sorting through the mess on worker productivity. At this point, it seems to me that the major issue is not that the Internet world is struggling to cope, but which product and approach does an organization choose to stop unwanted email? There are now hundreds of products claiming to solve the problem. How do you choose?

Solutions fall into two groups: those that filter the email to folders and those that challenge the sender. (There are other suggestions such as charging for email, but these are yet to be fully explored.)

Both have their merits; both have their faults. Filter technology is the dominant player. Many products use the same underlying process and produce much the same results; the real differentiation comes with performance, price and usability. Not many products use challenge-response and there are a number of articles to suggest that it is not a good solution.

I'd like to suggest that this is not a time for muddled thinking, but one for looking to the true benefits of Challenge-Response and accepting that it, like the other solution, is not perfect, but has benefits that the filter technology cannot match.

Forget you are an IT professional for a moment (if you are!) and sit in the end-users chair. Many end-users are getting 100-200 unwanted emails a day. They want to stop them. They don't want them to go to another folder that must be visually sifted for what is wanted and what is not. For example, there might be 2-3 genuine emails and a user must find these amongst all the others. Senders of genuine emails are not always savvy and sometimes include information that has the email identified as unwanted. Filter technology demands that the end-user check the folders as email in these folders is deleted after a time.

Challenge-response will stop unwanted email. The end-user simply doesn't get it. No folders to check, no filters to update, no hassles for the end-user and isn't that who we actually care about?

Remember again that you are an IT professional and let's look at the downside of challenge-response – there are plenty of articles on the Internet that go into it chapter and verse.

Most of the expressed downside is rubbish; for example, the “deadly embrace” of challenge systems talking to each other. There are three issues with challenge-response that I believe are genuine and deserve consideration. Of course, these must be viewed in the light of the greatly simplified task of email management for the majority of end-users; most end-users don't fall into the following categories and will welcome the reduction of daily workload afforded by challenge-response.

The first issue is that of the genuine first-time sender to an email address that is using challenge-response. In the circumstance of concern, there are many genuine emails daily and the end-user wants to receive them all. For example, the receiver might be employed by a sales organization; the sender might be sending a genuine request for a proposal. No sales organization on the face of this earth would want to make it harder for the sender.

The brutal fact is that unwanted email has already made the task harder for the sender. If the receiver has challenge-response, then the sender will get challenged; if the receiver has filtering, then the sender's email can be placed in a different folder and the receiver must find it there. Both systems potentially inconvenience the sender; however, challenge-response has the advantage that if the sender fails to respond properly to the challenge, the sender knows that the email has not been delivered. If the filter system incorrectly identifies the email as unwanted, the sender may never know that the email has been undelivered. It opens the gate to the question: “Did you get my email?” and the receiver can never positively answer “yes” or “no” when the receiver hasn't seen it. The solution for challenge-response lies in making the challenge and response a simple process for the sender. A number of non-email systems are now using the challenge approach and like most things that present immediate obstacles,

people later wonder what the fuss was about. Most senders are now sympathetic to the issues caused by unwanted email – aren't they also users? – and are not fussed about simple tasks that require authorization.

The second issue is the receipt of email from mailing lists. Challenge-response systems are designed to allow humans at the sending end to be authorized and to send email. Mailing lists are computer generated and these cannot respond to the challenge. Hence, it is up to the receiver to make sure that the sender's email address (or domain, or IP address, as the case may be), is authorized.

The problem only occurs when the user first joins the service, or when the service changes its sending properties. The solution for challenge-response lies in sensibly handling both these circumstances i.e. providing tools and facilities for the receiver to allow for receipt of wanted email from an unknown source and to be aware that list email is no longer being received.

The third issue is that senders can masquerade as legitimate senders in a receivers "white list".

Proponents of this objection correctly state that its not hard to find an address that is white listed and once found, the receiver has a complication; should the genuine sender be removed from the list to prevent the unwanted email? Challenge-response technology is not widely used at the moment, so that this issue is not yet a real threat, but it could become so. The solution lies in the implementation of a process to verify that the sender is who they claim to be (as determined in the protocol). There are a number of proposals from different vendors and research groups to address this need. Examples of these protocols are:

- Sender Permitted From (SPF),
- Designated Mailers Protocol (DMP) and
- Reverse Mail Exchange (RMX)

The Anti-Spam Research Group (ASRG) of the Internet Research Task Force (IRTF) is currently investigating these protocols to create a single standard. They are all simple to implement and can be done easily and gradually. When it's all said and done, it doesn't matter which approach is taken, but continued discussion will get the industry nowhere. End-users are looking to the industry to solve the problem and the only task remaining to beat Spam is that of legitimizing the sender.

I wrote before of the "benefits that the filter technology cannot match". What do I think these are?

Firstly, challenge-response enables the majority of email traffic to be rejected at the server. Current statistics suggest that 80-90% of email traffic is unwanted. Filter systems must read all this email to determine its characteristics and the increasing resources required for this process should not be underestimated. Challenge-response systems enable organizations to free up the network facilities; in particular, large organizations can free-up substantial resources for the management of legitimate traffic. In addition, there is the associated virus and useless attachment information that is no longer read.

Secondly, challenge-response systems do not join the "Spam" race. Filter technology demands that the filters remain ahead of the "tricks" developed by the Spam senders to bypass the filters. By definition, they will always be behind and the cost of filter maintenance is an inherent part of the approach.

Finally, challenge-response systems eliminate unwanted email. It's not filtered and quarantined, its rejected. The systems run themselves, so there is no central administration. There are no issues with "the filters were too strict or too loose", no false positives and no maintenance.

In summary, there may be some issues with challenge-response, but at the end of the day, it delivers. There is no unwanted email in the end users in-box.