

Sender Policy Framework
and
Challenge-Response

A Powerful Combination

Ben Corby
Technical Director
New Millennium Solutions Pty Limited
bcorby@totalblock.net
2 July 2006

Challenge-Response and Sender Policy Framework (SPF)

Challenge-Response stops all spam, but what is [Sender Policy Framework](#) and what does it offer to a challenge-response system?

Challenge-Response is a 100% successful method for stopping spam, which it does by issuing a challenge to the sender of an email from an unknown source. To verify that the sender of an email is not a spammer, Challenge-Response sends out a challenge email. If a spammer has used someone else's email address as the return address, then that challenge goes to someone who never sent the original email. The technique of using someone else's address from which to send spam is called "spoofing" and is a common spamming ploy. Of course, the spam mail never breaks through the Challenge-Response system, but because some other anti-spam systems - e.g. those that use filtering techniques - are fooled by spoofing, spammers will continue to use spoofing.

It would be an improvement if systems did not need to challenge an email that was spoofing someone else's email address. The result would be to stop our systems wasting valuable resources and to save innocent third parties' systems from receiving irrelevant challenge emails. **Sender Policy Framework (SPF)** is the latest evolution of several different standards designed to address this problem.

SPF fits neatly into the current architecture of the Internet.

All domains that use email publish the address of a server that can receive email for the domain. If this were not done, the domain would never receive any email and the address would be published by a mail exchange (MX) record. Sender Policy Framework is the logical extension of this: it is a way to publicise the address of a server that can send email for the domain. The SPF record is stored in the same place as the MX record. So the first step to implement Sender Policy Framework is to create an SPF record, and many systems have already taken this step. The second step is for any email server that receives email to look up the SPF record for the sending domain and confirm that the address of the sending server is allowed to sent from that domain. This step is more complicated and is the reason why SPF, which can be so effective, has been so long in coming.

SPF implementation has been hampered by the usual battle between the industry giants, who are each convinced that their own approach is right – and in some cases, quite profitable for them. The result, again, is that while the giants battle, the job does not get done. However, after many years of a complete inability to get its act together, the industry at large is now ignoring the giants and SPF implementation is growing apace. The sooner the better.

The combination of Challenge-Response and SPF will see the elimination of unwanted email in the foreseeable future.

Wholehearted industry take-up is key

The real issue for SPF is the same as for any other system that requires intelligent implementation by the Internet community. Many organisations will understand what is required and implement SPF properly and without fuss. Some larger organisations will feel they should comply, but make only a token effort to do so because of the

substantial effort involved within a company their size. Other organisations will feel that regardless of the industry trend, their own solution is more appropriate.

At present, it seems that less than 15% of the industry has implemented SPF and of those, about one-third have opted to implement the soft option, in which the domain responds with a "likely to be genuine" reply to a domain query.

It is still not possible to be black and white about a receiving server reaction to the results of an SPF query. Even if the query fails, it might be because there is a fault in the implementation for the sending server. SPF is a great idea that will require general industry support before the benefits are felt.

It means that Challenge-Response will continue to be the best method to control unwanted email. When SPF is implemented properly, the result will be a lowering of resource utilisation rather than reduced volumes of unwanted email.