What Email Forwarding Services Need to Know About SPF

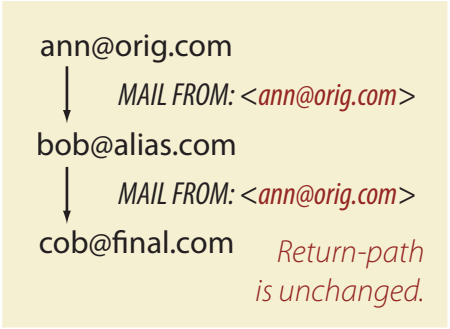
Worms, viruses, and spam forge envelope sender addresses in an attempt to disguise their origins. SPF, a new standard that exposes and rejects such forgeries, requires forwarders to rewrite envelope sender addresses. This document explains how.

January 8 2004 http://spf.pobox.com/srs.html

Meng Weng Wong <mengwong+srs@pobox.com> is founder and CTO of pobox.com, one of the first email forwarding services. He supports the SPF standard as a way to reduce the costs of spam.

To combat spams, worms, and viruses, the new anti-forgery standard called SPF adds a layer of protection to SMTP. When an SPF-aware MTA receives mail (from, say, *username@aol.com*), it asks the envelope sender's domain (*aol.com*) if it recognizes the IP address of the SMTP client. The domain publishes SPF records in DNS describing its outbound servers, as a sort of "Reverse MX" record. If those records do not describe the client IP, the MTA may reject the SMTP transaction as a forgery attempt.

SPF is stopping spam in the field today. AOL, for one, publishes records. Many major MTAs and anti-spam products, such as Postfix and SpamAssassin v2.70, are SPF-capable.



SPF presents a challenge to email forwarders. In classical email forwarding, the envelope sender address remains unchanged by the forwarder. But under SPF, a legitimate message that was forwarded through an intermediary might, unfortunately, be seen by the destination as a forgery. Forwarding services need to change with the times. Instead of preserving the original envelope sender, forwarding services now need to rewrite or encapsulate the sender address. The outbound message should bear a return-path showing the forwarding service, not the original sender. This is the best way to be compatible with SPF.

The return-path is used for bounce messages. If the target address is undeliverable, a bounce message is returned to the sender. Under classical forwarding, bounce messages are routed directly to the original sender. Under the new system, bounce messages are relayed back through the forwarding service, to the rewritten sender address. The forwarding service then unwraps the original sender and forwards the bounce. This illustration shows one possible form of Sender Rewriting.

In practice, you need to include a unique cookie in the new return-path that could only have been added by the intermediary. Otherwise, the forwarder would become an open relay, allowing spammers to make up addresses at the bounce-handling domain. To prevent replay attacks, those cookies should have limited validity and expire after a handful of uses.

Pobox.com developed the Perl module Mail::SRS to perform the Sender Rewriting Scheme described above. It is working in production for Pobox, and it has been released on CPAN. Other forwarding services are welcome to use it. No sense reinventing the wheel.

Many people are using SPF. Please implement Sender Rewriting soon.

If you need assistance implementing a Sender Rewriting scheme, you can contact mengwong+srs@pobox.com.