Andrew Rose posted a note in RISKS back in January 2004 alerting readers to a new project called SPF (Sender Policy Framework, <http://spf.pobox.com>) that uses "SPF records" to be published in the domain name system (DNS). E-mail sent with fraudulent headers would be identified because the sender would not match an authorized SMTP server registered in the DNS by means of these records. Rose wrote, "The technical work on SPF is now complete and adoption has started. Several thousand domains have published SPF records including some very large domains such as aol.com. Plugins exist for most of the popular MTAs - the only notable exception being MS Exchange." [MTA = Message Transfer Agent]

In a sharply worded riposte in RISKS 23.18, Markus Fleck-Graffe attacked the whole idea of SPF, pointing to these failings among others:

1) All forwarded e-mail must be rewritten (e.g., mailing lists must destroy the original header to substitute their own authorized domain);

2) Forwarded e-mails require a database of reverse mappings to allow bounce messages to reach the original sender;

3) Spammers will subvert the system by establishing their own SPF-enabled infrastructure using temporary domain names;

4) Worms will use the authentic e-mail addresses of their infected host PCs.

Also in RISKS 23.18, Ian Jackson criticized the SPF group for not using the IETF RFC mechanisms to stimulate discussion and improvements of the proposal but rather, "going for a publicity campaign to `bounce' people into adoption."

In RISKS 23.19, Lawrence Kestenbaum detailed the misery caused by spammers and worms that use his e-mail address in FROM lines, causing thousands of bounce messages to arrive at his address daily. He wrote in exasperation, "The critics of SPF suggest that spammers would simply find or invent other addresses to use. Frankly, I don't care about that, so long as they stopped plastering my personal address on hundreds of thousands of fraudulent and disreputable spam messages and viruses, and clogging my server's net connection with vast piles of misdirected bounces."

In RISKS 23.21, Ben Rosengart recommended doing away with the SRS (Sender Rewriting Scheme) part of SPF, leaving forwarded e-mail with the original header unchanged. Peter da Silva pointed out that "Implementing SPF would do nothing for the people receiving thousands of bounces (myself included). It would simply add another filter that bounced messages back to
us because 'we' weren't using the right server."

Dmitri Maziuk added to the conversation with the observation that "We know that slapping a band-aid onto implementation to fix deficiencies in design doesn't work and creates more problems…." He wrote, "We already have directory servers, we already have digital signatures. All we need is a way to query Domain Name Service for directory server of a domain, and a standard directory query-response for an e-mail address and associated public crypto key." He also darkly suggested that there would be resistance to this scheme from political forces who actually support spam for their own purposes: "…all "anti-spam" legislations are really there to legalize it. Ergo, all you're going to achieve by implementing SPF, blocklists, blacklists, whatever, is to open yourself to lawsuits from 'legal' spammers."

In RISKS 23.23, Jonathan de Boyne Pollard bitterly points out that SPF is a short-term move in an arms race and that it fails to solve the underlying problems of SMTP (which include failure to authenticate message origins). He ends, "…perhaps the fact that widespread adoption of SPF will do serious damage to the SMTP mail architecture is a good thing. In the battle against unsolicited bulk mail, we've concentrated upon the wrong problem time after time, with mechanisms that address the wrong thing and that don't address the actual 'unsolicited' and 'bulk' qualities of undesirable mail. SMTP has become less usable, more patchy, and more balkanised with each new bodge, yet continues to bend and not quite break completely. Perhaps the adoption of SPF will turn out to be the straw that finally breaks the camel's back, and that thus finally forcibly weans us off this bad habit of addressing the wrong problem."

The Wikipedia article on SPF <http://en.wikipedia.org/wiki/Sender_Policy_Framework> has a good review of the project, including a detailed summary of controversial aspects of the system. In addition, I found the November 2004 white paper <http://spf.pobox.com/whitepaper.pdf> by Meng Weng Wong of the Messaging Anti-Abuse Working Group an excellent summary of theory and implementation details. That paper’s interesting layout includes what could have been footnotes as comments and diagrams placed in a separate column on the right-hand side of each page. It makes for fascinating reading and is worth while for mail-system administrators.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www.msia.norwich.edu/> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.