Comment #: 24

From: Joel Rees
Sent: Wednesday, September 29, 2004 12:38 PM
To: Authentication Summit
Subject: comments for the Email Authentication Summit

In order for any sender authentication plan to function reliably and effectively, three elements must be in place:

First, some means of identifying the sender;
Second, a scarcity of maladministered mail servers and proxies (and clients);
And, third, a scarcity of server OSses that don't leak like sieves.

The first requirement is still not known to be achievable, after several hundred years of regular mail and over thirty years of electronic messaging. It can be almost achieved, as an exceptional method of transmission, and at a cost.

But where there is a machine, there is a way to emulate it. Automate it and incorporate it into the standard mail path, and those who have the desire to defeat have all the opportunity they need.

(In the case of e-mail, until Microsoft and other e-mail browser companies can control their bouts of featuritis enough to resist the temptation to add what are essentially virus and trojan APIs to their software, the malware transport system for spam will remain available.)

We can't afford to bring the mail delivery mechanism into the war of escalation which is security and encryption.

Rather than attempt to establish mandatory authentication as part of the transport, there is a far simpler method to handle spam. Take away the incentive, and much of the problem will go away.

When we need protection from physical junk mail, we often buy a post office box and only give the address for that box to the people we want to hear from. When we look through the POBox, we look at everything. When we look through the box on the front porch, we use a different scanning mode.

It really would not be much of a burden for e-mail providers to give out two or three mail addresses in their basic service, something like

jo-user@private.mailprovider.com
jo-user@news.mailprovider.com
and jo-user@junk.mailprovider.com

The customer could set filters to sort the several addresses out in her e-mail client. In addition, either the client software or the mail server could provide some extra mechanical assistance.

The junk address could automatically delete old mail when the volume goes above some limit. Although advertisers could feel free to send mail to the junk box, the smart ones would also be aware that the more they send the less the user is going to read. (To aid this process, the receiving end could even automatically sort the junk mail by sender.)

The news address could be set up by the user to bounce any mail not

from any newsgroup or mailing list she is not subscribed to. Spoofing the newsgroup/list server would be a probable problem, but might be ameliorated somewhat by included the IP address(es) of the source server as well as the domain name(s). This sort of thing would need some work, but might be worthwhile for newsgroups and mailing lists.

The private address could maintain a black/white list. Anything on the blacklist would automatically bounce, and anything else not on the whitelist would go to a holding folder (preferably visible to the user) while waiting for the sender to respond to a challenge. The challenge would be in the form of a message that says something like "put secret-word" in the subject and reply to get your original mail sent through.

Challenge mechanisms have the potential to turn into a repeating mechanism at present. A standard challenge header could short-circuit the feedback, if it were widely accepted and used.

These mechanisms are known, and are actually in use by many privately administered mail accounts. They work well where implemented.

Separate mailboxes will be a much more effective and much cheaper solution than authentication.

--
Joel Rees