Spam bounces considered harmful

Rodney Tillotson

The expectation that e-mail services will return a failure notice or report for messages that cannot be delivered is no longer realistic. In most cases Janet-connected organisations should not attempt to provide such notifications.

The Changing Environment

The traditional assumption on which the standards were based is that all mail is legitimate. Notifications were included as as to make e-mail services more “reliable”, so that anyone who sent a message could suppose that it would get to the intended recipient’s account unless a message of failure was sent back.

It is now necessary to presume that an e-mail message is guilty of abuse until proven innocent. In e-mail abuse the originator address is almost always false; it may be pure fiction, or it may be a valid address selected from some list but unrelated to the actual source of the message. All classes of abuse behave in similar ways: UBE (Unsolicited Bulk E-mail or “spam”) sent from a dedicated network or through stolen resources in insecure PCs (“zombies”, “bots”); viruses that propagate by e-mail; “phishing” campaigns.

Mail servers are, of course, configured not to simply deliver such abuse. They may notice what it is and suppress or (particularly for virus messages) delay delivery, or the target address may be invalid or temporarily unavailable. In such situations, notifications on the traditional model are likely to be misdirected.

Reject, Don’t Bounce

The standards provide for a mail server to “reject” a message by refusing its transfer, rather than accepting it and risking future problems.

The process for transferring a message between mail servers (for instance, one out in the Internet and one in a Janet-connected organisation) involves:

1. a TCP/IP network connection
2. some preliminary negotiation, mainly of e-mail addresses
3. the transfer of the data constituting the e-mail message.

At each stage the destination server either sends an acknowledgment, or terminates the transfer. If the pair of servers reach the data phase and the destination server sends an acknowledgment, it then becomes responsible for the message. Otherwise the destination server is said to have “rejected” the transfer attempt and need not generate a “bounce” or a warning. The sending server is left to decide what to do with the message.

Opportunities for Rejection

1. A destination server can apply a local policy at the connection stage using a list of forbidden IP addresses. They might be addresses belonging to known senders of UBE, consumer IP addresses likely to have viruses or zombies, or other insecure networks through which abuse may occur. The Janet RBL+ lists such IP addresses in a form recognised by most mail server products, and there are a number of other DNSBLs (DNS Block Lists).
2. The destination server may be able to reject a transfer on the basis of the originator e-mail address alone, if it has a non-existent or wholly undesirable domain. Once the server has both the connecting IP address and the originator domain, there are a number of proposed schemes for comparing the two. SPF (Sender Policy Framework) would record in the DNS which sending servers are legitimate for the originator address domain. Some mail server products can use SPF information, but deployment is at present patchy.When the server has the local address for message delivery, it should be able to reject messages for invalid or otherwise undeliverable addresses. This is relatively easy for small organisations with a single server, but in most networks in this community the server that needs to make the decision is not the one that will attempt delivery to valid addresses. There are a number of ways in which the outward-facing server can still test the validity of a destination address: it can send a dummy delivery request to the delivery servers; it can interrogate their user databases directly; or it can refer to a copy of the user database maintained as a file. It is harder to anticipate other problems such as “quota exceeded”, server misconfiguration, or the generation of out-of-office notifications at the whim of a user.
3. The message contents passed in the data phase can be examined and a responsed delayed, so that if the message contains indicators of a virus or UBE, the server can still reject the transfer. Not all mail server products yet support this, and integration of anti-virus products and UBE scanners with an outward-facing mail server is not straightforward. Dedicated appliances are available, but they may make it difficult o validate local destination addresses as above. DKIM (DomainKeys Identified Mail) would include a cryptographic signature in individual messages which can be verified at this stage with a key published in the DNS for the originating domain.

The aim for the operation and management of each organisation’s e-mail should be to reject unwanted messages without the need to generate bounces or other warnings. Where that is impracticable, servers must do what they can to identify classes of message for which notifications are suppressed. For instance, UBE or virus messages accepted by an outward-facing mail server and only later found to be for invalid addresses should be silently destroyed.

E-mail Users

If you are principally a user of e-mail rather than a provider, you may reasonably hope that the manager of your e-mail servers has done all they can to correctly reject whole classes of unwanted messages. You should treat with the utmost scepticism every remaining unexpected message, even if it appears to be from a postmaster or e-mail server and related to something that might concern you.

You should avoid doing anything with received messages which may cause irritation to third

parties. Use of vacation or out-of-office features, and forwarding of spam complaints using indiscriminate or naive programs, commonly lead to mistakes.

References

[1] RFC2821: [1](*Offsite link*)

[2] Janet RBL+: [2]

[3] SPF: [3](*Offsite link*)

[4] DKIM: [4](*Offsite link*)

Links
[1] http://www.ietf.org/rfc/rfc2821.txt?number=2821
[2] http://community.ja.net/library/janet-services-documentation/dns-block-lists
[3] http://spf.pobox.com/
[4] http://mipassoc.org/mass/