

Email Authentication Summit- Comments Matter Number P044411

Federal Trade Commission
Office of the Secretary, Room 159-H, Annex V
600 Pennsylvania Avenue NW.
Washington, DC 20580
authenticationsummit@ftc.gov

Key Points:

- An authenticated HELO domain is the only sufficiently strong name identifier within a mail stream to safely identify the message source and allow a reputation assessment of those accountable.
- The HELO domain is analogous to the letter postmark, but is currently unreliable due to a protocol defect resulting from limitations in DNS information. Without changes to RFC 2821, the HELO domain must be allowed to fail authentication.
- Adding a DNS Service record to assure HELO domain authentication and additionally validating authorization can be implemented without any negative impact upon existing applications.
- Making the authenticated HELO domain name visible to the user would be an effective and safe deterrent against phishing and spoofing, as this identity would be the most difficult to spoof as a means to provide false assurances.
- The authenticated HELO domain identifies the server holding the SMTP log needed for criminal enforcement.
- Authenticated HELO domains enable a simple and safe means to associate authorized mail transfer agents with the mailbox domain through the publishing of a simple name list. The alternative text scripts, as used with SPF or Sender-ID, to obtain addresses for a large array of hosts is inherently perilous, and must be discouraged.

Reduction in Spam

A strategy predominately used to reduce spam and preserve network resources is called the Real-time Black-hole List (RBL). This list is based upon the IP addresses of the connecting client where, when a record is returned after the address is queried, the client is refused with a reply that often names the list responsible for the rejection. The address is used as the identifier because there are currently no validated names associated with a mail stream. The lack of a validated name makes it difficult to know when an address has been reassigned and the reverse DNS name directory is too poorly maintained to be of use for this purpose as well.

An address is currently the only strong identifier that is authenticated by way of interaction within the transport protocol within a mail stream. With the potential number of addresses being fewer than the potential number of names, tracking addresses that are

