Comment #: 41

From: Keith Moore
Sent: Thursday, September 30, 2004 7:35 PM
To: Authentication Summit
Subject: Email Authentication Summit-Comments (Matter Number P044411)

I wish to submit the following comments in response to the FTC's request for comments in connection with its Email Authentication Summit, as announced in the September 15 issue of the Federal Register.

I am a Senior Research Associate at the University of Tennessee, Knoxville, specializing in networking protocols. I am an author or co-author of several IETF email protocol specifications, and have previously served as a co-Director for the Applications Area on the Internet Engineering Steering Group (IESG). I have also written a widely used program to facilitate the sending of bulk email.

No email authentication scheme that has been proposed has gained wide acceptance because each of the proposed schemes, if adopted, would seriously impair a significant class of users or significant legitimate uses of email. This has happened for a variety of reasons, ranging from a desire among certain players to gain a competitive advantage at others' expense, to a willingness by some proposers to remove valuable functionality from email protocols - for instance, the ability to submit mail from arbitrary locations in the Internet, or the ability to send mail from an arbitrary location using any of one's email addresses, or the ability to send mail on behalf of consenting third parties or consenting multiple parties.

For an authentication scheme to be useful in reducing spam and/or phishing, it must be widely adopted. For an authentication scheme to be widely adopted, it must:

- Be transparent to existing mail readers;

- Not semantically alter authenticated messages;

- Not significantly reduce valuable functionality. (For instance, there are several valid reasons for the From header field to differ from the administrative domain used to send the message);

- Incrementally deployable on existing platforms and without major disruption;

- Have no significant barriers to incorporation of the scheme in existing mail handling tools, including barriers related to licensing or use of patents or other intellectual property;

- Not rely on any single trust hierarchy, but instead allow recipients (or agents acting on their behalf) to determine which keys or certificate authorities they trust;

- Not significantly favor any provider or vendor of mail handling hardware or software, or operating system, over another;

It is also important to understand that authentication schemes are of limited benefit in reducing spam. The fact that many spammers today take measures to conceal their identities is a reflection of the hostility with which recipients react to spam. But this hostility

exists for two reasons: one is that the spam interrupts and interferes with valuable interpersonal communication; the other is that the content of the spam itself is frequently offensive.

Widespread adoption of a standard authentication mechanism could well _increase_ the overall amount of spam seen by consumers, except for those consumers who are willing to strictly limit (say, by explicit enumeration) the persons from whom they are willing to receive mail. Authentication would probably reduce the amount of illegal and highly offensive spam, but this is likely to be offset by an even greater amount of spam touting other products and services. While this might be seen as an improvement, an increase in spam would still impair use of email for interpersonal communication. On the other hand, authentication would likely reduce the amount of illegal spam and phishing, and these are desirable outcomes.

It is useful to separate two distinct goals that might be served by authentication of email. One goal is to allow the recipient to reliably determine whether the message was sent by someone who is known and trusted. A separate goal is to determine whether the part who sent the message can be held responsible for his actions in sending the message. Meeting the first goal impairs the ability to send anonymous mail. It also does little to reduce spam except for recipients who wish to strictly limit the parties who can send them spam. It is possible to make a message traceable without immediately disclosing the identity of the sender to the recipient - for instance by having a third party certify "I know who the sender is and I will reveal the sender's identity if this message meets certain conditions" (e.g. is spam, contains a virus, violates laws, or on the order of a court of appropriate jurisdiction).

It is possible, and to some extent reasonable, for multiple authentication schemes to coexist. Ideally, senders (or their mail submission agents) could authenticate a single message using multiple mechanisms, and recipients (or their incoming mail servers) could verify an authenticated message using any of the schemes used to authenticate it. The ability to support multiple schemes is in some ways highly desirable, because this facilitates transition from one scheme to another as (for example) market conditions and usage patterns change, or existing schemes are compromised (as does unfortunately happen sometimes) or new cryptographic mechanisms come into favor. However support for multiple authentication schemes does require some degree of commonality - for instance they must not use the same mail protocol elements in dissimilar ways, nor impose mutually incompatible restrictions on how the mail protocol is used. And it is preferable if only a small number of schemes are in widespread use at any particular time.

The handling of authenticated and unauthenticated messages will need to vary from one recipient to another, according to the degree with which authentication is adopted and according to each recipients' requirements. For instance, a person who corresponds with people all over the world may need to accept email from individuals regardless of whether they have authenticated their mail, or from countries in which authentication is not widely adopted, or where a server that revealed its senders' identities would violate local privacy laws.

The best way that the Email Authentication Summit could support standard-setting efforts would be to try to obtain agreement on a common set of design goals. It might also be useful to work toward an understanding by which multiple authentication schemes and/or multiple certificate hierarchies could peacefully coexist.