Comment #: 9

From: David A. Wheeler
Sent: Monday, September 27, 2004 11:43 PM
To: Authentication Summit
Subject: E-mail Authentication Summit-Comments

Here are my comments on email authentication per
your request in the Federal Register, Sep. 15, 2004.

My response is lengthy, but the fundamental issues
are simple:
* NIST should urge lawmakers to make spam illegal,
  so that technological measures will have legal standing.
  Authentication has little anti-spam value without it.
* NIST should insist that any anti-spam technical standard
  must be implementable by all suppliers of email
  infrastructure, both proprietary and open source software.

Thank you.

Here are the details:

In question 1, you ask: "Whether any of the proposed authentication standards
(either alone or in conjunction with other existing technologies) would result
in a significant decrease in the amount of spam received by consumers;"

By themselves, none of these authentication standards will
result in a significant decrease in the amount of spam, and
limiting solutions solely to technological measures will not
help either.

The fundamental problem is that our laws are
antiquated and have not yet caught up to Internet technology.
Fundamentally spam is theft, but one that the laws permit.
Spam steals 8 or more hours a month of my time; why am
I not paid for this theft of my time? Spam steals vast amounts
of computing resources; many organizations have to buy
larger hard drives and network connections solely because
of spam.

There's no point in worrying about authentication as long
as this theft is illegal. So what if it's authenticated -- it's
authenticated theft. As long as there is no legal way to
respond to the theft, authentication has no value.

Businesses must be able to accept emails from
strangers; it's how they get new business.
Home users must usually accept emails from
long-lost people they knew from years ago.
It's not practical to only accept email from previously

known email addresses. Thus, a spammer can create a new address for every message, each of which can be authenticated. And as noted in the Register, spammers now take over user's machines, and thus they can send email as that user (and could authenicate themselves, too).

This doesn't mean that authentication is useless. Authentication is useful in its own right, especially for countering phishing attacks, and for eliminating false "bounce" messages from forged email. And authentication, when combined with other anti-spam technology, could have a very slight impact on spam in the short term. But unless there are laws forbidding spam, that permit civil suits and recovery of damages against spammers, then the technological measures will not be very effective.

Once there are real anti-spam laws (instead of the current "you CAN-SPAM anytime you want to" U.S. laws), then authentication will be very useful, because it will help to track down lawbreakers. But as long as theft is legal, there's no reason to authenticate people who might not be breaking the law.

Laws are quite possible. The U.S. already forbids fax spam, and that law was passed for all the same reasons that email spam should be illegal. Europe has passed "opt-in" laws (instead of the worthless "opt-out" laws). Once most countries pass such laws, people can decide to simply refuse to accept email from other countries that don't have or don't enforce such laws.

The current laws are foolish. It has been clearly declared, for many years (and including IETF RFCs) that users should NEVER respond to so-called "opt-out" messages, since this clearly marks the respondant as a "real email address" that spammers will target even harder.

Don't believe the nonsense about it being impossible to define spam. Other laws have had definitional issues, and they've been created anyway. A simple rule would be sending essentially the same logical message to more than 1000 people without their prior consent (e.g., by signing up for an email message).

This group must recommend that laws be passed to forbid spam, and require OPT-IN (not OPT-OUT) to large lists. Then the technological measures will have a chance at being effective, since they can then help enforce laws instead of social conventions.

Question 3 asks about compatibility with existing software; questions 7-9 and 29 ask about control of the specification. All of these questions indirectly with a serious problem

that you have no doubt already heard: namely, that
one of the major proposals (Microsoft's) has been
cleverly designed to create market incompatibilities.

Microsoft is encumbering its proposal with what it
calls its "Royalty Free Sender ID Patent License."
Novices might see no problems with this, but
this is simply not a reasonable proposal.
As the careful analysis of Mark Shewmaker
(http://www.imc.org/ietf-mxcomp/mail-archive/msg03514.html)
and others shows, this license is extremely
discriminatory: it is essentially incompatible with
open source software (OSS).

Since vast amount of the mail
infrastructure is implemented with OSS,
this is unreasonable and extremely discriminatory.
For example, the Apache Software Foundation (ASF)
announced that it couldn't support Sender-ID, at:
http://www.apache.org/foundation/docs/sender-id-position.html
This is important since ASF releases the widely-used
SpamAssassin (as well as the Apache web server).

Any authentication system MUST be implementable
by all major systems. This means that it must
be implementable by all open-source and
proprietary systems. Mere public specification
is not enough; systems must be IMPLEMENTABLE
to be useful, and that includes terms that
permit widespread implementation by all
relevant parties.

Thus, as a private citizen I urge NIST to
clearly articulate that any anti-spam or authentication
standard must be clearly implementable by all
implementations, both proprietary and open source software,
or they should not be made standards.
If NIST makes this clear this would be a
useful result for question #29.

There are, no doubt, other important issues.
But I hope that you find these comments useful.
I wish you well in your deliberations.

--- David A. Wheeler