Comment #: 23

From: John Glube
Sent: Wednesday, September 29, 2004 1:14 AM
To: Authentication Summit
Subject: Email Authentication Summit-Comments, (Matter Number

September 29, 2004

Federal Trade Commission
Office of the Secretary,
Room 159-H (Annex V),
600 Pennsylvania Avenue, NW.,
Washington, DC 20580

Attention: Donald S. Clark, Secretary

Dear Mr. Clark

Re: Email Authentication Summit-Comments, (Matter Number P044411)

I understand the FTC is planning on holding an Authentication Summit in early November.

I applaud this effort by the FTC to work with the private sector in implementing a system wide domain level authentication scheme to help secure email and stop the scourge of email forgery.

This is important as I use email in my business to publish three newsletters, keep in touch with customers and generally to allow me to run my business.

One major concern. It is my understanding that Microsoft has filed two patent applications concerning sender authentication and due to the broad scope of the claims, any patent rights may cover sender authentication based on SPF's SMTP Mail From and Microsoft's Purported Responsible Address proposals.

To facilitate quick deployment, we need one or more open standards.

Since the majority of mail servers use open source software, if any open standard is subject to intellectual property rights, any patent or copyright license needs to comply with the Open Standards Alliance model.

In this case, based on the present position of Microsoft, this does not seem possible. We therefore run the real risk

of one corporation, which is presently the dominant player in the desktop market place, gaining control of a crucial part of the email infrastructure and in essence owning email.

In the circumstances, I urge the FTC to take all steps necessary to ensure:

* any standard involving domain authentication is open; and

* if subject to any intellectual property claims, any patent or copyright license be compatible with the Open Standards Alliance model.

Recently I published an article, which helps to explain the specific problems with the MARID proposals dealing with mailfrom and pra checking and sets out a solution:

For The Record, Will Microsoft Own Email?
http://www.learnsteps4profit.com/wme.html

Please consider this article as part of my comment.

In this way, the private sector can protect its interests, while avoiding any anti trust concerns, so allowing for an even competitive field.

At the same time, the FTC is ideally suited to facilitate the private sector in moving ahead with designing and deploying one or more open standards for sender authentication.

Given the importance of the world-wide email and DNS systems, any scheme for domain authentication likely to see broad deployment must contain no mechanisms that would have deleterious effects on the overall system.

I am paraphrasing the review standard recently set out by the IESG for the proposed technical directorate, after closing the MARID working group.

As you may be aware, the IESG decided:

* the WG Chairs and Area Directors ask the editors of existing working group drafts to put forward their documents as non-working group submissions for Experimental RFC status; and,

* The Application Area Directors set up a technical directorate to conduct a focused technical review of the proposals, based on the referenced standard.

Once this process is complete, to my understanding the IESG will then review the submissions, along with the technical review and decide which, if any submissions be put forward as an IETF sponsored experimental proposal, subject to an Internet wide last call.

I believe a number of the questions raised by the FTC and NIST in its register notice, given the discussions on the MARID list, reflect the need for a detailed and focused technical review of draft-ietf-marid-protocol,

draft-ietf-marid-submitter, draft-ietf-marid-mailfrom, draft-ietf-marid-core and draft-ietf-marid-pra.

In the interim, the SPF community continues to forge ahead both with deployment and design, including a new proposal for a responsible submitter that uses SMTP mail from checking, to create a cleaner "work around" for mail forwarding, along with apparently working on a protocol document for HELO checking.

At the same time, I reference for your benefit the Compatible Low-level Email Authentication and Responsibility (ietf-clear) proposal which to the best of my knowledge is not encumbered by any intellectual property rights.

This pre-IETF charter working group has been set up to pursue SMTP envelope authentication techniques, derived from CSV and BATV.

To my understanding, the initial input documents are draft-ietf-marid-csv-intro, draft-ietf-marid-csv-csa, draft-ietf-marid-csv-dna, and draft-levine-mass-batv.

I gather at least csv-intro, csv-csa and csv-dna have been subject to an operations and security review by the "graybeards," senior IETF members who make themselves available to conduct initial focused technical reviews.

For more information on CLEAR:

http://mipassoc.org/ietf-clear/index.html

Trusting these comments are of assistance. Should you have any questions concerning this submission, please do not hesitate to contact me at your convenience.

Yours truly

John Glube
Glube's - Business Services

Canada