Open letter to the Federal Trade Commission

November 10, 2004

Chairperson Deborah Platt Majoras
Federal Trade Commission
Room 440
600 Pennsylvania Ave, NW
Washington, DC 20580

Commissioner Orson Swindle
Federal Trade Commission
Room 540
600 Pennsylvania Ave, NW
Washington, DC 20580

Commissioner Thomas B. Leary
Federal Trade Commission
Room 528
600 Pennsylvania Ave, NW
Washington, DC 20580

Commissioner Pamela Jones Harbour
Federal Trade Commission
Room 326
600 Pennsylvania Ave, NW
Washington, DC 20580

Commissioner Jon D. Leibowitz
Federal Trade Commission
Room 340
600 Pennsylvania Ave, NW
Washington, DC 20580

Director Arden Bement, Jr.
National Institute of Science and Technology
100 Bureau Drive
Mail Stop 3460
Gaithersburg, MD 20899

Dear Chairperson Majoras:

The SPF Community is a recently formed group, established to represent the interests of the SPF community and to carry forward with the work of email authentication as represented by the Sender Policy Framework. This community is comprised of many of the people who have been actively involved in developing this framework.

We applaud the effort by the FTC and NIST to work with the private sector in implementing one or more system wide domain level authentication schemes to help secure email and aid in thwarting the scourge of email forgery.

The potential real world effects of email authentication on the online community are significant. Great strides have been made over the last 10 years in developing a highly efficient email infrastructure. Unfortunately, the plague of unsolicited bulk email, along with the spread of viruses and trojans has reached crisis proportions, threatening the continued viability of email as a communications medium.

It is imperative that the online community as a whole tackle these problems We must work together in bringing those who abuse email under control. But prudence is important in carrying out these efforts.

- Technological means can only go so far in controlling online social problems.
- The implementation costs of any authentication proposal must not outweigh the real or perceived benefits.
- The email infrastructure is complex, having grown organically over the years. Care must be taken to ensure any proposal easily fits within this structure without breaking any of its parts.
- The vast majority of those who work and play online are not truly computer literate. Therefore any authentication methods must be robust and easy to implement.

Presently there are various proposed methods of email authentication.

IP/Domain based authentication

IP/Domain based authentication relying on the Sender Policy Framework (SPF) or Sender ID Framework (SIDF) allows for last hop validation.

The benefit of this approach is that it combines mail channel authentication using the fully qualified domain name (FQDN) found in SMTP MAIL FROM and message authentication using the Purported Responsible Address (PRA) Algorithm.

However, initial studies suggest these approaches may impose significant overhead requirements.

Compatible Low-overhead Email Authentication and Responsibility (CLEAR) focuses in part on mail channel authentication and domain accreditation using the IP address, based on the FQDN found in the EHELO/HELO command. This allows for end to end validation and accreditation, while apparently imposing less overhead requirements.

Cryptographic Methods

At the same time, light weight cryptographic approaches seem to afford a better approach to allow for an effective mechanism to properly verify whether to send a non-delivery report or delivery status notification (Bounce Address Tag Validation [BATV]).

Also, it is perceived validating RFC 2822 from (in particular Identified Internet Mail - CISCO and DomainKeys - Yahoo!), so allowing for message authentication may be best carried out using cryptographic methods.

The Crisis

The online community's frustration with the spam epidemic and especially the dramatic rise in phishing has created a crisis atmosphere.

Proceeding Forward

Given this crisis, there is a strong desire in certain circles to simply proceed with one IP/Domain based approach to provide an immediate response to the dramatic rise in phishing attacks.

However, all of the IP/Domain based proposals are experimental in nature. In shutting down MARID, the IESG stated in part:

"The working group chairs and Area Advisor intend to ask that the editors of existing working group drafts put forward their documents as non-working group submissions for Experimental RFC status. Given the importance of the world-wide email and DNS systems, it is critical that IETF-sponsored experimental proposals likely to see broad deployment contain no mechanisms that would have deleterious effects on the overall system. The Area Directors intend, therefore, to request that the experimental proposals be reviewed by a focused technology directorate."

Accordingly, this process should be carried out as quickly as possible.

At the same time we can proceed with testing of the various approaches on a wider scale to verify or disprove existing views, develop the required code in some cases, work out any bugs and, where possible, simplify the implementation process.

Once testing is completed a better analysis can be conducted of the competing methods. Based on initial analysis and the complexity of the email infrastructure, it is quite likely that a layered approach is required. This analysis can then guide the community in selecting the proper methods and making the needed investment in Internet wide deployment.

Another concern is that some of these schemes are subject to intellectual property right claims. To ensure wide spread deployment and an equal playing field, we would urge that any licenses be royalty free and fully compliant with the Open Standards Alliance model.

In addition, work is required on the accreditation (reputation) front. However, the ISPs need to be prepared to work with the various proponents.

Unfortunately the lack of an industry standard for establishing consent to receive solicited bulk email continues to cause problems. In essence, with the largest direct marketing association in the United States advocating an opt-out approach, mail box providers are obliged to respond by letting their customers decide what is or is not spam.

This means a senders reputation is evaluated against a subjective standard, making it difficult to proceed with reliable approaches for accreditation (reputation).

The FTC and NIST can play a fundamental role in assisting industry to sort through acceptable technical guidelines for establishing consent. This will aid in ensuring that the process of establishing and maintaining a reputation is as objective as possible from the sender s and receiver's perspective.

We recommend the following:

- The editors of the various IP/Domain based working group drafts submitted during MARID follow the IESG directive and put forward their documents as non-working group drafts.
- The IETF Area directors proceed to form the focused technical directorate.
- The technical directorate carry out its work as quickly as possible with the full co-operation of the respective editors.
- Once this is done, the IESG proceed forward with its process of determining which proposals should receive RFC Experimental Status.
- While this work is ongoing, the major ISPs can gear up to conduct large scale tests over the upcoming months. At the same time smaller networks, along with individuals should be given the opportunity to participate.

- The results of these tests be made available to the participants. The FTC and NIST can then convene a workshop in the new year with participation from all stakeholders to review these tests and consider the next stage in the process.

- At the same time, significant education is required to aid the community at large in moving forward. For example, while some may consider the process of publishing an appropriate email policy record using the SPF syntax is quite simple, given the various ways of sending email, it can be complex even for those with relatively straight forward business environments. The FTC and NIST can assist in this process by working with the proponents in producing the needed guides and easy to use tools to aid the community in implementing the various protocols.

- The FTC work with the United States Patent & Trade Mark office and those claiming intellectual property rights to ensure all claims are properly brought forward and any licenses for use of core technologies are non-discriminatory, royalty free and compliant with the Open Standards Alliance model to allow for wide spread deployment. This is especially important, given that open source software predominates throughout the email infrastructure.

- The FTC and NIST monitor developments on the accreditation front. ISPs and others need to be prepared to work with a number of providers. The FTC can encourage this process so that accreditation does not form a market barrier, while at the same time raising levels of online compliance.

In the interim, the NIST can facilitate the ISPs in implementing the required technologies to allow for validation of financial web sites as suggested in the 2nd OECD Workshop on Spam Report to help deal with phishing attacks, so protecting all consumers while the community works on testing, analyzing and implementing email authentication.

To date industry has been unable to settle on standards for consent, given the wide range of views. The FTC and NIST can facilitate the process of establishing standards by working with senders and receivers in establishing technical requirements.

We appreciate this is a rather long list of recommendations. Email now forms an important part of our way of life and a fundamental element in operating an online business. We trust that you will give consideration to our comments and suggestions.

We thank you for your attention to these matters.

Yours truly,

The SPF Community

/jbg