Comment #: 2

September 24, 2004

George Mattathil

CA

To:

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

Subject: Email Authentication Summit—Comments,
(Matter Number P044411)

TO WHOM IT MAY CONCERN,

I have invented an anti-spam technology that is simpler and more effective than the proposed authentication standards, This technology is called "**Email Sender Verification (ESV^{TM}) System**" (patent pending). The key concepts in the ESV system are:

(1) Ability to trace (as opposed to authenticating) the sender of an email is sufficient for an effective anti-spam solution. Once it is possible to trace senders of spam, existing anti-spam laws can be enforced.

(2) Completely solving the spam problem after the emails are in the in-box is not possible. So emails have to be made distinguishable as non-spam before they are sent.

(3) ESV system targets the solution on the email sender-side before legitimate emails are sent. All ESV-enabled emails will carry a tamperproof ESV-tag. Incoming emails are inspected for the ESV-tag. If the ESV-tag is present and valid, then the email is automatically sorted as legitimate. Emails without an ESV-tag are sorted into a separate category. As ESV adoption increases, the percentage of legitimate non-ESV emails will drop rapidly. As the benefits of sending spam decline, it is possible that spam email may cease to be an overwhelming problem as it is now.

(4) The key features of the ESV technology:

a) An overlay over the existing Internet email infrastructure

b) Backward compatible with current Internet email systems

c) Based on open architecture

d) Optional and voluntary use.

(5) Only email users who do not wish to receive and send spam need to adopt the ESV system for it to be an effective solution (those who are sending spam need not use it for the system to be effective). If those who send spam use it, they will become traceable and anti-spam laws can be enforced.

(6) Once the adoption issues are overcome, the ESV system could become a feature of existing email products/services (and no longer required as a separate product/service).

(7) The ESV system enables the email users to determine policies, and use patterns affecting their email addresses and identities. Incorporation of optional centralized administrative oversight and/or management is also possible. The implementations of the email user policies use patterns may be centralized by email service providers, or implemented on the email user's computer -- with email users having primary control. Aggregation of the policy and use pattern implementations may be domain-based, by responsible entity, or based on administrative convenience.

(8) A patent application has been filed for the *ESV technology*. Several implementation variations of the technology are possible. Developing an uniformly acceptable standard (*ESV standard*) for anti-spam applications is a logical choice. A system that implements the ESV technology is an *ESV system*.

Response to Request for Comments

Comments below relate to the issues listed in Section C, Request for Comments, of the FTC notification -- with respect to the ESV technology.

Issue 1. An ESV (verification) system alone is sufficient to significantly decrease the amount of spam received by consumers.

Issue 2. ESV system does not require authentication, but only verification -- trace-ability of the email sender (hence simpler).

a) ESV system does not require Certificates, public-key, or PKI.

b) ESV system does not require any modifications of the current Internet or email protocols.

Issue 3. An ESV (verification) standard would require additional software, but will work with any existing hardware that is compliant with current Internet and Internet email protocols (SMTP, POP3, IMAP, etc.).

a) Cost of ESV software will be comparable to that of current anti-spam software.

b) ESV software is optional. However, users not using the ESV software will not have its benefits.

c) ESV software can be made available for download through an Internet website (ESV portal).

Issue 4. An ESV (verification) standard has no impact on the operators of receiving email servers, unless they choose to implement ESV as part of their email services. If operators of receiving email servers do not implement ESV, then the email recipients can implement the solution and get the benefits of ESV.

Issue 5. An ESV (verification) standard will be 100% reliable if both the sender and recipient use it -- no false negatives or false positives. Here are the different usage scenarios:

	ESV Sender	ESV Recipient	non-ESV Sender	non-ESV Recipient
ESV Sender	n/a	100% effective	n/a	same as now
ESV Recipient	100% effective	n/a	some improvement	n/a
non-ESV Sender	n/a	some improvement	n/a	same as now
non-ESV Recipient	same as now	n/a	same as now	n/a

Table 1. ESV Usage Scenarios

Issue 6. The ESV (verification) system is mutually exclusive to all authentication standards. An ESV standard will interoperate with all non-ESV systems that are compliant with current Internet and Internet email protocols.

Issue 7. The ESV (verification) technology can be implemented as an open standard, with the standard specifications made public. (Specifications need not be secret for the ESV system to be effective.)

Issue 8. The ESV technology is patent pending.

Issue 9. Use of the ESV technology will be protected by applicable patent laws.

Issue 10. An ESV (verification) standard has no impact on email forwarding services.

Issue 11. Mobile users could potentially gain all the benefits of the ESV (verification) standard. ESV systems are domain-neutral.

Issue 12. Roving users could have all the benefits of the ESV (verification) standard, provided all service providers are compliant with current Internet and Internet email protocols.

Issue 13. Adaptations for mailing lists can be incorporated into ESV (verification) systems.

Issue 14. Outsourced email users could have all the benefits of the ESV (verification) system, provided all the service providers are compliant with current Internet and Internet email protocols.

Issue 15. ESV (verification) systems are transparent to multiple apparent responsible identities, without any reduction of benefits.

Issue 16. ESV (verification) systems are transparent to web-generated email, without any reduction of benefits for email users.

Issue 17. ESV (verification) system is scalable -- added computational overheads are negligible.

Issue 18. Computational complexity of an ESV (verification) standard is same as software currently in use, and contains no features to make it technologically impractical.

Issue 19. An ESV (verification) standard can be implement as two software components:

(a) ESV email client software component

(b) ESV server software component.

Current industry pricing models can be adapted for ESV systems. For example, An ESV email client software could be made available for free Internet download, with priced versions with enhanced features. And ESV server software priced similar to industry practices.

Issue 20. By marketing the ESV solution directly to consumers, there is a reasonable chance for rapid adoption of an ESV systems.

(a) The ESV (verification) standard will be transparent to ISPs who do not participate in the ESV (verification) standard.

(b) No implementation schedule exists at present.

(c) An initial estimate for the development time for a working version of the software components is 3-6 months.

Issue 21. An ESV (verification) system will add a small delay (in microseconds or milliseconds) per email, depending on network delays and processor speeds -- but will be not be noticeable to email users.

Issue 22. The ESV (verification) standard will permit consumers to engage in anonymous political speech. Consumers may turnoff the ESV system at will, or use a verification level that is appropriate for the communication. (Similar to sending postal letter -- bulk mail, first class, certified, certified with return receipt, etc. -- with, without return address or dummy address, as applicable).

Issue 23. Antitrust safeguards are prudent for an industry-wide authentication standard, as with any situations that has potential antitrust implications due to "network effect" (Applications that have community elements, when usage reaches certain critical threshold, tend to increase significantly or magnify the barriers for entry of new products and entrants).

The driving motivation of the Internet pioneers was to improve human communication by means of computers (“Galactic Networks”). Openness and simplicity were the results, with email being the best example. Spam is a result of abuses of this communication media, designed with openness as an overriding criteria. If the original intentions for the Internet are preserved in the public policies and related regulations, antitrust problems are unlikely to be an issue for an anti-spam standard.

Recommendations

(a) Establish well defined public interest position to maintain Internet and Internet email as a public communication media/channel.

(b) Establish well defined public interest position to maintain Internet and Internet email to Open Standards (interoperability with alternate systems with backward compatibility).

(c) One of the key requirements for email to be an effective communication media/channel is *Assurance of Delivery* -- senders need to have the assurance that their email will reach the intended recipient. Unfortunately, some of the anti-spam solutions do not adhere to this principle. To appreciate the importance of *Assurance of delivery*, imagine what would happen if the postal service did not operate on the principle of assured delivery.

Issue 24. Users of ESV (verification) standard will be able to monitor and prevent unauthorized use of their email address and identities with automated software tools. However, abuses of email addresses and identities may continue on non-ESV enabled systems, without impacting users of ESV systems.

Issue 25. Users of ESV (verification) system will be able to prevent "phishing". However, "phishing" of non-ESV users may continue.

Issue 26. ESV (verification) system does not need any authentication schemes. Hence do not have the complexity associated with authentication systems. An ESV system will be very similar to any other software package that requires installation and simple management actions as and when needed. Eventually, the critical elements of the ESV system could become features of email products and services for simplified use.

Issue 27. The ESV (verification) standard will allow implementation of different verification schemes in different jurisdictions -- transparent to users -- without sacrificing interoperability, decrease in benefits or increase in complexity.

Issue 28. An anti-spam ESV (verification) standard do not need any new cryptographic standards to solve the current spam problem. However, it may use existing or new cryptographic schemes for enhanced and/or differentiated verification levels.

Issue 29. Spam is the result of the abuses of a public communication medium/channel, namely email. Therefore, Email Authentication Summit would better serve the consumer interests by addressing the problem within a policy framework for the email medium, and help develop:

(a) Policy guidelines

(b) Email system requirements (mandatory and optional)

(c) Email service requirements (mandatory and optional)

(d) Email system and service interoperability requirements (mandatory and optional)

(e) Facilitate commercial partnerships and agreements that can allow the emergence of promising new solutions.

(f) Establish a financing scheme to help overcome the "Capital Gap" for commercializing promising new solutions, either through a public-private partnership or a publicly funded program.

Issue 30. Adoption of standards and products based on technical merit and consumer benefits.

(a) Establish a public-private monitoring and regulating body to ensure that the consumer, public, small business, and commercial interests relating to the Internet and Internet email are protected. And promote the development of new, innovative and beneficial consumer applications of the Internet and email technologies.

Please contact me if you wish to receive additional details about the ESV technology, and/or have other questions.

Yours truly,

George Mattathil