



Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
<http://www.cisco.com>

October 20, 2004

Information Society Directorate-General
European Commission
BU 24 0/41
Rue de la Loi 200
B-1049 Brussels

Re: Questionnaire on the Implementation of the Communication on Unsolicited Commercial Communications or "SPAM" (COM (2004) 28)

Dear Commissioner:

Cisco Systems, Inc. ("Cisco") is pleased to have the opportunity to provide our responses to your questionnaire on unsolicited commercial communications.

In October 2003, Cisco decided to work on a technological approach to spam. We developed the Identified Internet Mail authentication framework, and are currently advancing it through the Internet Engineering Task Force ("IETF"). We have attached the current draft of the Identified Internet Mail proposal with this response as a separate document. Cisco undertook this work because of the growing cost of spam to email users generally, to Cisco's customers, and to Cisco itself.

Many organizations concerned with spam are looking at authentication systems as an important tool to address the spam issue, including the Organisation for Economic Co-operation and Development ("OECD") and the United States Federal Trade Commission ("FTC"). An effective authentication system will give users and system administrators the ability to choose to implement policies to reduce spam, reduce the requirement for multilayered filtering and excess storage, improve latency, and allow more flexibility and choice regarding email.

Spam is often sent using techniques designed to disguise the true source of the message. The Simple Mail Transfer Protocol ("SMTP") permits senders to use any return address that they wish. This typically impairs attempts to shut down the spammer. In some cases, spammers can also disguise the identity of infected systems sending messages. An authentication system that includes the addition of a cryptographic signature to a message

will limit the opportunity of spammers or malware (worms, viruses, etc.) to forge return addresses and, thus, provides a reasonable degree of accountability for the source of email messages.

Cisco's signature-based authentication proposal, Identified Internet Mail, describes backward-compatible extensions to the format of email and a public-key infrastructure to permit verification of the source of messages by either mail transfer agents (MTAs) or mail user agents (MUAs). The intent of Identified Internet Mail is to determine if the sender of the message is authorized by the administrator of the domain to use a particular email address. A signature created using a private key is added to the message as a header and is subsequently verified using the sender's public key. The Identified Internet Mail proposal is flexible in that any required changes are transparent to mail users. A complete description of the proposal and how it works is provided in the attached IETF draft.

An important design goal for Identified Internet Mail is to preserve the positive aspects of the user experience in the current email infrastructure. This includes the ability for anyone to communicate with anyone else without introduction, the ability to send an email from outside one's home domain, and the retention of current characteristics of anonymity.

We believe that authentication approaches such as Identified Internet Mail will provide a solid foundation to reduce spam.

Cisco looks forward to continuing to participate in the Commission's work on this important subject. Cisco understands that the Commission services plans to hold an open workshop on spam, provisionally scheduled for 15 November 2004, to discuss the contributions received and the possible way forward. Cisco would be pleased to participate in the workshop and share our views on authentication and technology approaches to reduce spam.

Thank you for the opportunity to provide these comments. We would be happy to discuss these issues further or clarify any responses. Please feel free to contact Pastora Valero at +32 (0)2 704-5344 for this purpose.

Sincerely,

Cisco Systems, Inc.
Sanjay Pol
Vice President

Questions

1. Self-regulatory actions

1.1 *Has your organisation adhered to, or developed, a self regulation code with regard to unsolicited commercial communication or spam? (please specify)*

As a global participant in internetworking technologies, Cisco is an active proponent and user of technologies to combat spam. Cisco's approach to protecting our own network is based on detecting and marking unwanted email messages at incoming mail servers. We scan various parts of all incoming mail to determine if they match any known patterns of spam. Messages that appear to be spam based on initial filtering are then run through a series of additional filters to determine with greater certainty if in fact they are spam. Filtering and deleting spam at the incoming mail servers also reduces the security risks of introducing worms, viruses, and other malware into our network. Cisco regularly monitors and evaluates new products and technologies, and works actively with other industry participants, to further improve spam detection and elimination.

1.2 *How have your contractual practices towards subscribers and towards business partners with regard to spam changed since implementation of the e-Privacy Directive (2002/58/EC) in the EU?*

These comments are focusing on Cisco's Identified Internet Mail authentication solution. We do not address the above issue in this response.

1.3 *Can you provide information on filtering techniques and software in use internally or offered by your company to customers (including ISPs)?*

Cisco believes that the increase in spam has largely been made possible by the ability of spammers and malware to spoof return addresses, that is, disguise the true source of messages by changing the return address in Simple Mail Transfer Protocol ("SMTP"). When the source of spam is difficult to identify, it is difficult to shut down or isolate.

To address this issue, Cisco has proposed to the Internet Engineering Task Force ("IETF") a signature-based mail authentication standard called Identified Internet Mail. The full text of the Identified Internet Mail draft proposal can be found at <http://www.ietf.org/internet-drafts/draft-fenton-identified-mail-01.txt>. The proposal is designed to help identify fraudulent messages and apply a user-defined policy before it is accepted by the receiving domain. Identified Internet

Mail provides the tools for administrators and users to implement policies that are appropriate to their environment. For example, an un-authenticated message can be marked as such and treated in the same manner as current email messages. Authenticated messages may be treated preferentially with respect to their routing, prioritization, and content filtering.

Using Identified Internet Mail, a recipient of email messages can verify that the sender of a message is authorized to send messages using a given email address and also verify the integrity of the message. This makes the sending domain more accountable for email messages originating from their domain and limits the ability of spammers and malware to forge return addresses or disguise the identity of infected systems. Authentication also serves as a foundation on which existing and future accreditation and reputation services may be based. We expect the market to drive these systems, or others, as a further step in addressing spam.

The Identified Internet Mail specification is backward compatible with current email infrastructure and allows a graceful migration to authentication. The changes that the proposal will require are related to the application of a signature to outgoing mail and the verification of signatures on incoming mail. Signature verification is done by using specific entries to the Domain Name Service (“DNS”) server or through a new web server, called the Key Registration Server (“KRS”), within the sending domain. A KRS is a simple web server application where the public key verification function replies to a request by a recipient domain.

No changes to the mail protocols, such as SMTP, are anticipated. Further, since Identified Internet Mail is signature based, there is no technical limitation that impacts the user’s ability to retain current characteristics of anonymity or choose any email name they may wish to choose.

To understand how Identified Internet Mail compares with other approaches, we address the three common categories of spam and email fraud solutions:

- (i) Content filtering
- (ii) Path-based / source IP-address verification
- (iii) Signature-based verification

Content filtering solutions, which are based on the analysis of subject, header, text, images, or other content, represent a reactive approach because they attempt to identify spam after a message has been received. As a result, while end users may experience a decline in spam, the volume of spam to the network may increase as spammers attempt to get a small number of messages through the filters. Enterprises will have to absorb the added cost of network and email infrastructure that they will need to manage the increase in traffic. In addition, there may be added costs to update content filters and some users may experience

the blocking of legitimate mail messages that may contain some of the content being filtered.

Path-based approaches use mechanisms that allow the receiving domain to determine if a mail message originates from the domain that it purports to. The verification process involves querying the sending domain to check if the IP address from which the message was received is in fact authorized to send mail messages from that particular domain. Various forms of black listing and other policies may then be applied to determine the disposition the message based on the source IP address.

Source IP address-based verification is easy to implement but has some non-trivial limitations. First, this approach is susceptible to IP address spoofing, a common technique used by spammers. Second, source IP verification may not work in situations where the message follows multiple hops, as is the case with mailing lists and affinity email addresses, before it reaches the receiving domain. And finally, source IP address verification is generally applied at the domain level and would be difficult to scale if adapted for use at the per user level.

Signature-based approaches use mail signatures to verify the authorization of a given sender to send email from a given domain. The goal of this approach is to identify the sending domain or user and allow the recipient to apply policies to accept or take other action depending on the outcome of the signature verification process. The addition of a signature to an email message significantly limits the ability of spam and fraudulent email senders' attempts to spoof their true source.

1.4 Do you take steps to block spam at the source? Please mention if you employ some of the following techniques and a generic evaluation of their usefulness:

- *preventing users from sending outgoing mail via any third-party mail-hosting services, limiting the rate of outgoing mail per user, authentication of sender mail, payment of mail services (to limit amount of total mail sent).*

Please see previous responses.

1.5 Do you take steps to block spam coming from other service providers? Please mention if you employ some of the following techniques and a generic evaluation of their usefulness:

- *rate limiting (maximum number of e-mails received by the destination e-mail server within a given timeframe), provide a 'reputation system' (a mechanism for destination e-mail server to determine if it should receive the incoming e-mail based on the known reputation of the source e-mail*

server), doing a checksum (a mechanism for the destination e-mail server to determine if an incoming e-mail is of bulk nature (i.e. spam)).

Cisco does not rate limit, provide a reputation system, or perform a checksum with respect to spam from other service providers.

1.6 *Do you offer your customers anti-spam filtering facilities? Which of the following techniques (static, adaptive, reputation system) do you employ?*

Please see our response to question 1.3 for an overview of the proposed solution.

1.7. *Please mention any other correlated actions which are being undertaken by your company.*

Please see previous responses.

1.8 *Do direct marketing practices in use or endorsed by your company/association adhere to specific, legally compliant methods to collect personal data (e.g., 'double' or 'confirmed' opt-in systems) that go beyond the opt-in regime foreseen by the Directive? (please specify)*

These comments are focusing on Cisco's Identified Internet Mail authentication solution. We do not address the above issue in this response.

1.9.1 *Are effective codes of practices in place that are opt-in compliant, in co-operation with the Article 29 Data Protection Working Party or competent national authorities where appropriate? (please specify)*

These comments are focusing on Cisco's Identified Internet Mail authentication solution. We do not address the above issue in this response.

1.9.2 *Has your organisation considered recommending the use of labels for opt-in compliant e-mails and databases to help users (and filters) recognise them? (please specify)*

These comments are focusing on Cisco's Identified Internet Mail authentication solution. We do not address the above issue in this response.

1.9.3 Have you used self-regulatory complaints mechanisms and alternative dispute resolution mechanisms (ADR)? (please specify)

These comments are focusing on Cisco's Identified Internet Mail authentication solution. We do not address the above issue in this response.

We have no comments on the questions in Section 2, 3 and 4. In these comments, we are focusing on the Identified Internet Mail authentication technological approach to reducing spam.

Thank you for the opportunity to provide this contribution.