



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

September 30, 2004

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

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

Dear Mr. Secretary:

Cisco Systems, Inc. ("Cisco") is pleased to respond to the Federal Trade Commission's (the "Commission") and the National Institute of Standards and Technology's ("NIST") Request for Comments in connection with the planned Email Authentication Summit of November 9-10, 2004. Spam is an important issue, and the Commission's decision to sponsor an Authentication Summit provides a useful public service which will increase the understanding of the role authentication can play in reducing spam.

In October of 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"). Cisco undertook this work because of the growing cost of spam to email users generally, to Cisco's customers, and to Cisco itself. An effective authentication system should give users and system administrators the ability to choose features which will reduce the requirement for multi-layered 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. This typically prevents attempts to shut down the spammer. In some cases, spammers can also disguise the identity of infected systems sending messages. Since the Simple Mail Transfer Protocol ("SMTP") permits senders to use any return address they wish, 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 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). This proposal is flexible in that the required changes are

transparent to the end user and signing and verification of signatures takes place through a trusted MTA, using keys which are authorized by the domain administrator.

The intent of Identified Internet Mail is to determine if the sender of the message has authorization (from the administrator of the domain) for the use of an email address. A signature, created with a private key is associated along with the corresponding public key is placed in a message header. The receiving domain can then verify the signature in the header of the message.

An important design goal for Identified Internet Mail is to preserve positive aspects of the user experience in the current email infrastructure, including 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 ability to retain current characteristics of anonymity.

We are pleased that the Commission and the NIST are holding the Authentication Summit in November. We believe that authentication is a solid foundation for making significant progress to reduce spam.

Our responses to the questions asked in the Request for Comments are as follows:

1) 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.

At present, the majority of spam uses spoofed addresses, incorrectly claiming to be from a different address. Authentication mechanisms are designed to detect messages generated using spoofed addresses and therefore should help reduce spam. 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. Developments in authentication technologies, and the market response to reduce spam, lead us to be optimistic that spam, fraudulent, and malware-generated messages can be significantly reduced.

2) Whether any of the proposed authentication standards would require modification of the current Internet protocols and whether any such modification would be technologically and practically feasible.

Signature-based approaches like Identified Internet Mail and Yahoo! DomainKeys require backward-compatible extensions to the headers of email messages, as well as additions to Domain Name Service (DNS) records. No changes to the mail protocols, such as SMTP, are anticipated.

- 3) Whether any of the proposed authentication standards would function with the software and hardware currently used by senders and recipients of email and operators of sending and receiving email servers. If not, what additional software or hardware would the sender and recipient need, how much would it cost, whether it would be required or option, and where it would be obtained.**

The Identified Internet Mail proposal was designed with a goal of maintaining backward compatibility and allowing a graceful migration to the new standard. It will work within any existing infrastructure but will require a few additions relating to the application of a signature to outgoing mail, and the verification of signatures on incoming mail. To accomplish verification of the signature, one can either apply a small software change to the DNS server or deploy a new component termed 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.

- 4) How operators of receiving email servers are likely to handle un-authenticated messages.**

Identified Internet Mail's design goal is to provide the tools for Internet Service Providers, enterprise customers, and consumers to implement policies that are appropriate to their environment. The actual policy implemented is at the discretion of the email administrator and recipient. For example, during the initial deployment of any of the proposed authentication standards at Cisco, un-authenticated messages could be marked as such, and would most likely be treated in the same manner as current email messages. Authenticated messages may be treated preferentially with respect to their routing, prioritization, and content filtering steps.

- 5) Whether any of the proposed authentication standards could result in email being incorrectly labeled as authenticated or unauthenticated (false negatives and false positives), and the steps that could be taken to limit such occurrences.**

With regard to signature-based approaches such as Identified Internet Mail, there is a small risk of false positives because modification to the message in transit may cause the signature to not verify successfully. However, this risk is mitigated through the use of canonicalization algorithms that take into consideration likely in-transit modifications and eliminate elements such as spacing from the signature calculation. Identified Internet Mail has incorporated canonicalization schemes that may be chosen by the signer of the message.

- 6) Whether the authentication standards are mutually exclusive or interoperable. Whether any of the proposed authentication standards would integrate with any other standards. For example, if Mail Server A is using standard X, will it accept email easily from Mail Server B that is using standard Y?**

Each of the proposed authentication standards specifies a unique means for either path-based authentication (SPF, SenderID) or signature-based authentication (Identified Internet Mail, DomainKeys). The syntax used by the different proposals precludes direct interoperability within a given approach (e.g., DomainKeys interoperating with Identified Internet Mail); however, a path-based system and a signature-based system could be used in tandem as the systems utilize different mechanisms for message verification. They are complementary.

- 7) Whether any of the proposed authentication standards would have to be an open standard (i.e., a standard with specifications open to the public).**

It is essential that specifications for authentication be open to the public in order to achieve the wide deployment that is needed for email authentication to succeed.

- 8) Whether any of the proposed authentication standards are proprietary and/or patented.**

Cisco has at least one pending patent application relating to the Identified Internet Mail proposal. If Identified Internet Mail is adopted as an industry standard, Cisco is committed to making this patent available, if issued, on terms that permit wide acceptance.

- 9) Whether any of the proposed authentication standards would require the use of goods or services protected by intellectual property laws.**

With respect to Identified Internet Mail, please see the response to question 8.

- 10) How any of the proposed authentication standards would treat email forwarding services.**

Mail addressed to users via email forwarders should verify correctly with signature-based mechanisms. For example, Identified Internet Mail's user-based signature approach enables the user to send messages with a key issued or authorized by the forwarding domain, and allows the verification of messages received via the forwarder. However, path-based approaches do not have this flexibility since messages received via the forwarder do not take a direct path from the sender to the recipient.

11) Whether any of the proposed authentication standards would have any implications for mobile users (e.g., users who may be using a laptop computer, an email-enabled mobile phone, or other devices, and who legitimately send email from email addresses that are not administratively connected with their home domain).

Both the Identified Internet Mail and DomainKeys signature specifications accommodate this use case through per-user granularity of keys, as well as the ability to have the key reside on a Mail User Agent (MUA). This would permit a user's mobile device to be explicitly authorized to send mail on behalf of the user's home domain, regardless of the domain to which the mobile device is connected or the path the message takes.

12) Whether any of the proposed authentication standards would have any implications for roving users (i.e., users who are obliged to use a third-party submission service when unable to connect to their own submission service).

This use case is addressed by the same capability as the mobile user case discussed in question 11. A signature based approach (preferably with user-level keying) is required to authenticate the message when a third-party submission service must be used.

13) Whether any of the proposed authentication standards would affect the use of mailing lists.

Identified Internet Mail has mechanisms to preserve the behavior of mailing lists with little modification. Identified Internet Mail messages can contain signatures associated with the Sender or From addresses, or both. This allows mailing lists which re-originate messages and apply a Sender header (but retain the original From address) to sign the re-originated messages. However, since it is the From address that is most commonly seen by the recipient, it is important that if the Sender address is used to verify the message, the Sender address must be made visible to the user by the MUA.

14) Whether any of the proposed authentication standards would have any implications for outsourced email services.

With either the path-based or signature-based approaches, the domain may delegate authority to send messages on their behalf to outsourced mail services and other outsourcing providers. However, since many domains may be reluctant to give a third party broad authority to send messages using any address in the domain, the ability to authorize senders at a per-user level of granularity is more likely to be widely accepted. This is only possible with signature-based approaches. Additionally, such authorization

