Comment #: 32

CISCO SYSTEMS

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 may be assigned for a fixed time period and may be set to expire at a certain date. This could be particularly useful to authorize an outsourced email marketing campaign.

15) Whether any of the proposed authentication standards would have an impact on multiple apparent responsible identities (e.g., in cases where users send email using their Internet Service Provider's SMTP network but have their primary email account elsewhere).

Identified Internet Mail supports the current ability of mail to accommodate multiple responsible identities. While it is possible with path-based approaches for a domain to authorize Internet Service Provider SMTP servers to send email for the domain, doing so would likely also authorize every other customer of the same Internet Service Provider to send mail from the domain as well. Signature-based approaches permit the user to apply a signature prior to submission to the ISP and therefore do not have this problem.

16) Whether any of the proposed authentication standards would have an impact on web-generated email.

Identified Internet Mail can handle web-generated email in a couple of ways. If the web application has a private key which is authorized for the From address being used, it can sign the message directly. If mail is being sent on behalf of a user for which it does not have a key, it can list its own address in the Sender header of the message and sign the message on its own behalf. This would be useful for applications such as email invitations and forwarding of articles on the web.

17) Whether the proposed authentication standards are scalable. Whether the standards are computationally difficult such that scaling over a certain limit becomes technologically impractical. Whether the standards are monetarily expensive due to hardware and resource issues so that scaling over a certain limit becomes impractical.

Identified Internet Mail's design objective is to make the protocol scale easily. Identified Internet Mail specifies a separate key-management function, the Key Registration Service (KRS), which is a lightweight key verification procedure. Key Registration Servers, since they are web-based, can take advantage of scaling and load distribution facilities for web servers. This is computationally less intensive than the content-inspection methods of spam detection in operation today. The Domain Name Service can also be used for key verification, taking advantage of systems in place for redundancy, caching, and resiliency. For both techniques the load for larger domains should plateau because results of key authorization checks can be cached, resulting in better performance with scale.

18) Identify any costs that would arise as a result of implementing any of the proposed authentication standards, and identify who most likely would bear these costs (e.g., large ISPs, small ISPs, consumers, or email marketers).

Identified Internet Mail has been designed to be flexible and inexpensive to implement. In order to implement Identified Internet Mail, the expected additional costs are:

(a) At the sending domain: Software which creates message signatures may be deployed on an existing MTA, or alternatively deployed on a new hardware appliance based on the domain administrator's choice.

(b) At the receiving domain: Software which verifies message signatures may be deployed on an existing MTA, or alternatively deployed on a new hardware appliance based on the domain administrator's choice.

(c) The use of a Key Registration Server is recommended for larger domains but may not be necessary for smaller domains where the key lookup can be performed within the existing DNS infrastructure.

19) Whether ISPs that do not participate in an authentication regime would face any challenges providing email services. If so, what types of challenges these ISPs would face and whether these challenges would in any way prevent them from continuing to be able to provide email services.

ISPs that do not deploy authentication solutions would, of course, still be able to provide email services. However, to the extent their customers demand the benefits of authentication, and the ISPs do not respond, customers might switch to providers that could meet that demand.

20) Whether an Internet-wide authentication system could be adopted within a reasonable amount of time. Description of industry and standard-setting efforts, whether there is an implementation schedule in place and, if so, the time frames of the implementation schedule.

Signature-based authentication proposals, including Identified Internet Mail, are currently at the pre-Working Group level in the IETF. The pre-Working Group is expected to meet in November. After that, we anticipate that a formal Working Group will be established which will then work through the various signature-based approaches.

The demand for implementing the appropriate solution is strong, and one can reasonably predict wide implementation. The key to rapid adoption is the availability of software to perform the authentication and verification.

21) Whether any of the authentication standards would delay current email transmission times, burden current computer mechanisms, or otherwise adversely affect the ease of email use by consumers.

We expect that the implementation of an effective authentication standard will lead to faster email transmission times and cost savings. The email infrastructure today contains filtering mechanisms for anti-spam content analysis which add several seconds or minutes to the overall email latency. In addition, the reduction of overall traffic due to decreased spam should lower server and communication loads.

22) Whether any of the proposed authentication standards would impact the ability for consumers to engage in anonymous political speech.

Since the Identified Internet Mail proposal is signature based, there is no technical limitation that impacts the user's ability to retain their anonymity or to choose any email name they may want to use.

23) Whether any safeguards are necessary to ensure that the adoption an industry-wide authentication standard does not run afoul of the antitrust laws.

Should a standard be adopted that requires the use of Cisco's intellectual property related to its Identified Internet Mail proposal, Cisco will make it available on terms that ensure widespread adoption.

24) Whether a spammer or hacker could compromise any of the proposed authentication standards by using, for example, zombie drones, spoofing of originating IP addresses, misuse of public/private key cryptography, or other means.

Best practices in security employ defense in depth, and can ameliorate potential problems with zombies. These practices can include the use of tools that detect a compromised PC and implement security policies such as the isolation of the offending computer.

Additionally, signing at Mail Transfer Agents provides the MTA operator (usually the ISP) with the ability to observe the rate and volume of outgoing messages, and potentially halt outgoing messages if a PC is exhibiting anomalous behavior.

Finally, a message signing system allows the tracing of zombie behavior definitively to the sending domain, allowing more efficient identification of compromised machines.

25) Whether any of the proposed authentication systems would prevent "phishing," a form of online identity theft.

Today, a large percentage of phishing occurs by the sender crafting a message falsely appearing to come from a known domain, e.g. a bank. The application of Identified Internet Mail allows the bank to state that all messages it sends will have the bank's signature, and any message without such a signature or with an unverified one would be invalid. Such fraudulent mail would not carry a valid signature and receiving domains should be instructed that such unauthenticated, or wrongly authenticated mail should be discarded. This would prevent the end user from ever seeing such a phishing attack. Over time as existing phishing techniques evolve, so will the defenses, but in almost every case authentication will provide a more secure state.

26) Whether the operators of small ISPs and business owners would have the technical capacity to use any of the proposed authentication standards. Whether any of the authentication standards could be reasonably implemented by smaller ISPs.

Deployment of Identified Internet Mail is relatively simple and flexible in that it can often be implemented via a "plug-in" to a domain's MTAs. Key management may often be provided via DNS records or via a web server configured to operate as a Key Registration Server (KRS). This depends on the size of the domain, the need to provide user-level keying, and administrative preferences.

27) Whether any of the proposed authentication standards would have cross-border implications.

As with all Internet standards, the proposed email authentication standards are global in nature and are being considered in the recognized global standards body for the Internet.

28) Whether any of the proposed authentication standards would require an international civil cryptographic standard or other internationally adopted standard and, if so, the implications of this requirement.

Please see the answer to question 27 above.

29) Description of how the Email Authentication Summit can support industry or standard-setting efforts.

The Email Authentication Summit is benefiting the industry and the standards process by bringing together leading experts in a thoughtful way to openly share views on this important topic. As a proponent of industry-wide standards, Cisco Systems applauds the effort and looks forward to the Summit.

30) Assuming a domain-level authentication system is established in the near term, future measures that the private market should develop and implement in order to combat spam.

Email users and domain owners have significant incentives to reduce the cost of spam. Authentication systems will result in cost savings and efficiency benefits for users including increased productivity and reduction of storage and filtering requirements.

Identification of the sender 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.

Thank you for the opportunity to provide comments. We would be happy to discuss these issues further or clarify any responses. Please feel free to contact Adam Golodner at 202 661-4013 for this purpose.

Respectfully submitted,

David Rossetti
Vice President, Strategic
Software Technology
Cisco Systems, Inc.