Cisco Systems, Inc. (“Cisco”) is pleased to respond to the Federal Trade Commission’s (the “Commission”) Request for Comments in connection with the planned Spam Summit of July 11-12, 2007. Spam continues to be an important issue for e-mail and for the Internet as a whole, and the Commission’s decision to sponsor this summit to follow up on its previous related summits in November, 2004 and May, 2003 indicates the Commission's continued interest in finding some relief for this problem.

Cisco has been working on technological solutions related to the spam problem since at least October, 2003. Our initial e-mail authentication proposal, Identified Internet Mail, was merged with Yahoo!'s DomainKeys technology, resulting in the DomainKeys Identified Mail specification, which was very recently approved as a standards-track protocol (RFC 4871) by the Internet Engineering Task Force (IETF). Cisco is active in promoting e-mail authentication, and in specifying policy mechanisms that indicate domains' use of authentication.

The topics listed for discussion at the Spam Summit cover a wide range, from technology to social issues and from individual users to large service providers. Accordingly, we have chosen to provide comments on only those topics on which Cisco has particular insight or experience.

Defining the Problem

As a large enterprise, Cisco has been exposed to a considerable and much increased volume of spam over the past few years. Messages that successfully make it through our corporate-level spam filters appear to be increasingly fraudulent and deceptive, and are frequently a delivery vector for malware.

While several years ago Cisco's e-mail infrastructure performed filtering cautiously in order to minimize false positives, the increased volumes have necessitated more aggressive filtering. We expect the threat to continue to evolve and present a challenge to emerging filtering technologies.

Looking forward, the increased use of e-mail authentication can be expected to result in the use of "disposable" domains, which are domains that are registered in order to obscure the identity of the registrant, or to discourage establishment of a negative reputation for a domain. Even though domain-based reputation services are just being established, Cisco has already seen evidence that these “disposable” domains are being used to send authenticated e-mail. As e-mail authentication becomes more widely deployed, we expect this trend to continue.

Deterring Malicious Spammers and Cybercriminals

In order to make the messages they send appear more credible, cybercriminals are likely to send messages using e-mail authentication. Fortunately, this will limit the their ability to use arbitrary source addresses, and they will need to either register domains from which to send their messages, or use whatever authenticated addresses might be available from a compromised computer.

The use of e-mail authentication by cybercriminals will provide an additional forensic tool that can be used by law enforcement. However, it is important that other weaknesses in the identity chain be strengthened since they are the likely next avenue of exploit. In particular, additional controls on the registration of domain names will be needed to improve traceability of “disposable” domains that might be used by cybercriminals.

Emerging Threats

One of the primary characteristics of e-mail that contributes to its abuse is the lack of a central point of control. However, this is also one of the keys to e-mail's usefulness and scalability.

Other messaging services that can be expected to evolve into a similarly decentralized or federated model are the likely victims of next-generation abuse. To date, instant messaging (with the notable exception of XMPP) has been characterized by individual, centrally-managed services. Voice services are more likely to federate, which makes them more likely to be abused.

Enterprises are beginning to open their messaging infrastructure, including voice, video, and instant messaging (IM), with business partners and managed service providers. As this scales to more and more such partners, federation of these networks is likely. Since the cost of entry to voice and IM networks is approaching zero, these networks are likely to be subject to similar abuse as the e-mail system. In addition, such new modes of communication will lead to new modes of social engineering.

We can therefore expect these threats to increase. Authentication will be important to provide accountability for messages and limit the ability of social engineers and cybercriminals to abuse these new modes.

Putting Consumers Back in Control

E-mail authentication is an important mechanism by which consumers can be put back in control of the messages they choose to read. E-mail authentication provides information to a message recipient to help decide whether to open a given e-mail message. The presence of a verified signature from a known brand should provide a consumer with the confidence that the message indeed originated with that domain.

One of the issues that complicates consumer control of messaging is the research that indicates that consumers often make poor choices: even with existing content analysis solutions, consumers have been shown to open messages from "junk" folders, and click on links found therein. This has led to the development of policy mechanisms through which domains might seek to have unauthenticated messages blocked from delivery to consumers. Provided that the underlying authentication mechanisms can achieve a low "false alarm" rate (legitimate messages being seen as unauthenticated), these policy mechanisms are likely to be beneficial. However, consumer education will still be needed for the great majority of e-mail domains that cannot or do not publish these strict policies.

Technological Tools for Keeping It Out of the Inbox

One of the primary difficulties with keeping spam out of the inbox has been the relative unreliability of the primary tool, content filtering. E-mail authentication, although also not 100% reliable, provides an additional tool when used with accreditation and reputation based on the authenticated e-mail domain. Reputation systems can be as simple as a locally-maintained whitelist of known e-mail correspondents, or as sophisticated as centrally-managed reputation services. Accreditation services might be established among specific vertical markets such as banking, or might involve a fee-funded service that audits mailing practices by domains and grants (and revokes as necessary) accreditation to domains observing best practices for e-mail.

Open, standards-based solutions for both authentication and for publication of accreditation and reputation data are essential to wide deployment of such services. Interoperability between senders and verifiers of authenticated e-mail is required for the authentication system to work at all. Similarly, accreditation data is likely to be published by a number of providers, and verifiers need a consistent format for interpreting that data.

Stakeholder Best Practices

With the emergence of standards-based e-mail authentication, it is important that e-mail providers act quickly to provide authentication for outgoing messages, and to check incoming messages for authentication. As they become available, the addition of reputation and accreditation checks will greatly enhance the ability of recipients to categorize messages as spam or desirable. Finally, it is important that providers provide flexible mechanisms to act on the result of these checks, by rejecting messages where the sender's policy and recipient's preferences permit, and making the result of these checks visible to recipients in other situations.

Jim Fenton
Cisco Distinguished Engineer
Technology Center

Cisco Systems, Inc.
CA
USA
www.cisco.com