Comment #: 26

From: Xesdeeni
Sent: Wednesday, September 29, 2004 1:19 PM
To: Authentication Summit
Subject: E-mail Authentication

Here's a vote for the DomainKeys technique. I believe this would be more compatible with the SMTP system than the Sender ID, and avoid any potential hijacking of IP addresses, especially for e-mail relaying.

Answers to your questions:
1. In the 10's of thousands of SPAM I've received, I have not seen any that would not have been stopped by the DomainKeys technique.
2. I believe no modification of the Internet protocols would be required.
3. I believe the DomainKeys technique would be completely compatible with current hardware and software. Enabling the system would require software modification, but a system without the modification would still function correctly.
4. Receiving e-mail servers are likely to dump unathenticated messages. However, piping the message back to the originating IP might be preferable. While the possibility of IP hijacking mentioned above could change things, this type of "complaint" would quickly inform offending server owners of the problem.
5. Both Sender ID and DomainKeys would incorrectly label e-mail with return addresses through e-mail forwarding services as unauthenticated.
6. It appears that both Sender ID and DomainKeys are incompatible with some current e-mail forwarding services. In many cases, effectively, a user spoofs their own return address.
7. All e-mail standards should be open standard to ensure compliance, and to encourage widespread adoption.
8. It appears that the Sender ID technique is encumbered by patents and/or is proprietary.
10. It appears that the DomainKey technique would be compatible with e-mail forwarding servcies, since the sending domain would not need to be online or directly connected to the recieving server for authentication.
11. The DomainKey technique appears compatible with mobile users.
12. It does not appear that either Sender ID or DomainKey would be compatible with users who use a 3rd party submissing service.
13. The DomainKey technique should be compatible with mailing lists, where the list server validates incoming e-mail, and the receivers validate the list server.
15. Both Sender ID and DomainKey appear to have problems with "multiple apparent responsible identities."
16. DomainKey appears to be compatible with web-generated e-mail.
17. While DomainKey requires more resources than

current e-mail, by cutting down on the ever-increasing amount of SPAM, the overhead is negligible compared to current resource use.
18. The sending and receiving servers should already be sufficient to handle DomainKeys. While generating the digital signature is more overhead than current e-mail servers have per e-mail, the huge number of SPAM eliminated would more than make up for this overhead.
19. ISPs that do not participate in the authentication of receiving e-mail would risk their customers being the focus of SPAM as other ISPs deflect the onslought. Those that do not participate in the authentication of outgoing e-mail would risk themselves being used as a source of SPAM and being blacklisted (amputated) from the web. This is the absolutely desired outcome!
20. The adoption of any authentication system relies on the authors of the most used e-mail server software including it (enabled) in their new releases. If that is done, quick adoption (within a year) by almost all the Internet is likely.
21. As mentiond above, if there were no SPAM, DomainKeys would be a burden on servers, slow e-mail, etc. But SPAM does much more damage now, so the virtual elimination of SPAM would net a huge improvement in server burden and e-mail response.
22. Anonymous political speech is not a right via e-mail. My inbox is not a public forum, and just like no-one is allowed to invade my home to give a political opinion (particularly wearing a mask!), their intrusion on my e-mail is not allowed. Anonymous political speech and discourse can be held in blogs, on web sites, and even on Usenet...all public forums.
24. Any system can be circumvented by running programs on the servers themselves, such as "zombie drones." Spoofing IP addresses will not affect the DomainKey technique.
25. "Phishing" would not be affected by any authentication. Most "phishing" relies on URLs, which can already be traced. But "phishing" relies on human interpretation. www.citi-bank.com is not the same as www.citibank.com. An e-mail originating from the former would be validated, and thus delivered, just as it would be today. So the danger would not be affected.
26. Small ISPs would update their e-mail server software and the DomainKey technique would be enabled for them.
27. The cryptography used by DomainKeys may have cross-border implications. However, since the contents of the messages are not themselves encrypted, it is very possible that the use would not be an issue.
28. Any standard requires an open standard. Whether that standard is adopted in the U.S. and other countries follow, or an international committee needs to create one does not matter. However, it is unlikely the former will take longer than the latter.
30. In the future, coupled with the DomainKey technique, black listing of the holdout domains that

do not participate in authentication, black listing (now tracable) domains that support SPAM, and putting a huge penalty on even a single SPAM e-mail, would heavily curtail SPAM for the forseeable future.

Xesdeeni
