Combination of Envelope Return Address and Peer Network Address Provides Adequate Identity Validation for the Pay2Send Network of E-Mail Relays.

12th December 2002

Cryptographic signatures and extensive modifications to standard electronic mail protocols are not required to implement a working and practical system that only accepts incoming e-mail from known and validated senders of e-mail. While working on implementing the pay2send system, I have discovered that most senders of e-mail tend to favor particular "outgoing post offices" that they send their outgoing e-mail through, and that furthermore, the set of individuals with access to any particular outgoing post office machine is small enough that forgery may be considered an acceptable risk, and that furthermore, strong control on access to outgoing post offices exist so that is possible for the operators of an outgoing post office to be able to offer a guarantee that envelope return addresses on e-mail originating from a particular box are accurate.

The attached drawing D1 represents a situation in which a Sender "sender" who uses machine #1 is able to send a message to a Recipient "recipient" who uses machine #5 but a liar "liar" at machine #6 is not able to misrepresent themself as "sender" because of the invention, which is installed and operating on machine #3 in the drawing. This invention does not prevent Liar from misrepresenting himself as Sender if he is able to insert outgoing mail in machine #2, Sender's post office: that functionality is adequately provided by other mechanisms. Referring to drawing D1, blocking the 6-to-2 transmission of a forged message is outside the scope of this invention; a method of blocking messages from 7 to 3 while allowing messages from 2 to 3 is claimed.

E-mail post offices tend to have unchanging network addresses, and this tendency is relied upon by the validation method under description. When a pay2send relay, by which is meant an e-mail relay machine which is part of the system of pay2send network relays, receives an e-mail transaction, it knows the envelope return address provided for the message and it knows the network address from which the message arrived or is arriving. The software on that relay machine consults a database in which are stored a list of all registered (return address, peer network address) pairs, hereinafter referred to as RAPNAPs.

If the RAPNAP formed by the data from the message under consideration appears in the database, the message is considered to be from a valid sender and processing of the message continues on a track towards the recipient. Otherwise, the message is deferred. the pay2send relay may store the RAPNAP in a second database, under a hard-to-guess key, and e-mail that key to the return address for possible return to register this new RAPNAP as valid.

background and context about the pay2send relay system

The pay2send relay system is a system for limiting e-mail relaying to participating recipients, by allowing messages from "whitelisted" senders through, and also allowing messages from non-whitelisted senders through if the senders are willing to pay the recipient's receival fee. The pay2send system, which is under development by David Nicol's TipJar LLC, uses RAPNAPs to validate identities of e-mailsenders.

Claims:

1. The use of the combination of return address and peer network address (RAPNAP) to form a hard-to-forge identity key
2. Use of the above-described recognition method to automatically bill senders of e-mail, who have registed in advance, for use of a relay service.
3. use of the above-described recognition method to deny relay services to e-mail messages that do not come from verified sources

How to set this up, in suffiecient detail for a competent practioner in the art of writing e-mail Mail Transfer Agent software to implement the invention:

the remote mail transfer agent (MTA) network address is available at the time of the connection made to transfer e-mail, and is also available afterwards, written into Received: lines in an e-mail header. The envelope return address is the first piece of data transferred when an e-mail message is transferred.

way 1: Create a MTA that checks a database of known senders and the relay machines they customarily use and issues temporary failure codes, refusing to accept messages until the senders validate themselves and have deposited money into the system to cover their relay bills.

way 2: Create an e-mail postprocessor or delivery agent that analyzes header lines provided by an existing MTA and relays or does not relay messages based on the pay2send criteria.

sender thresholds and recipient fees

Each participating e-mail recipient in the pay2send system sets a fee that they require paid before they will receive an e-mail from a sender who is not on their whitelist. Each participating sender sets a threshold of what fee they will pay as a matter of course in sending messages. When the threshold is greater than the fee, and the sender has money on deposit in their pay2send account, the message is transferred and the pay2send money accounting system debits the sender and credits the recipient the recipient's fee. When the fee is too large, or the sender does not have funds in their pay2send account, the message gets deferred into the pay2send queue.

4. Claimed: the fee and threshold system described above

the pay2send queue

Pay2send relays store a queue of deferred e-mail. Each participant's incoming or outgoing messages waiting in it are called their incoming or outgoing queues. Participants are both recipients and senders.

Recipients can choose to inspect messages from their incoming queue, delete messages from their incoming queue, approve senders (or mailing lists) represented in their incoming queue, accept the offered fee for receiving a message from the incoming queue, all through a convenient user interface, such as an HTML form with a line on it for each message in the incoming queue and options concerning what to do with each message in a "select" input control.

Senders can choose to delete messages from their outgoing queue, agree to pay a fee higher than their usual threshold, by using a similar, or another part of the same, convenient user interface.

5. claimed: interfaces providing functionality listed above

the pay2send network

All the e-mail relays participating in the pay2send project will comprise the pay2send network.. They will communicate queued message information over to-be-determined internal communications channels and have secure channels to the central pay2send money accounting system. Also they will jointly maintain the global RAPNAP list.

6. Claimed: pay2send services may be distributed for high availability and high performance and administrative convenience.

7. Claimed: pay2send services for recipients at a particular e-mail domain may be provided on the e-mail post office machine that already handles the mailboxes for that e-mail domain

the global RAPNAP list

to encourage participation in the pay2send project, pay2send will make the RAPNAP database available via unlistable DNS, using software similar to what

is used to maintain the "realtime blackhole lists" of e-mail machines that have been compromised by bulk e-mailer nuisances. It is expected that the RAPNAP entry for, say, "nicold@umkc.edu sends messages out using network address 134.193.143.159" may get encoded into the global RAPNAP list as the appearance of a DNS record for nicold.at.umkc.edu.via.159.143.193.134.rapnap.pay2send.com following current best DNS practices.

8. Claimed: the RAPNAP database

9. Claimed: using domain name service to distribute the RAPNAP data.

To limit participation in the project to subscribers only, the pay2send project may withold the RAPNAP database except to registered dues-paid participants.

10. Claimed: witholding RAPNAP data from non-participants

mailing list servers

Good mailing list software creates a unique return address for every message it sends out, and these return addresses are only used once. The pay2send network recognizes this, and pay2send MTA software treats mailing list traffic as a special case. By identifying mailing list messages and keying on other aspects of them, such as identifying the RAPNAP information in the mailing list header, the pay2send system continues to work..

11. Claimed: parsing RAPNAP data out of headers in mailing list messages works when the mailing list software is reliable and consistent in placement of RAPNAP data.

12. Claimed: a set of additional sender preferences concerning automatically paying for messages sent through mailing lists or not

13. Claimed: recipients can whitelist mailing lists

14. Claimed: recipients can whitelist whole mailing list servers

Groups of servers with similar function

high-volume e-mail sites will often use multiple post offices, each with its own network address, to handle the high outgoing load.

15. Claimed: The pay2send system includes a mechanism for administratively joining multiple machines to reduce redundant RAPNAP registrations

More use cases:

There are lots of possibilities for e-mail addresses that cost money to send to:

16. Claimed: use of the pay2send network to sell a demographicly selected opt-in mailing list

17. Claimed: use of the pay2send network to demand a share of monies collected in the previous claim

18. Claimed: use of the pay2send network to filter communications to busy professionals

19. Claimed: use of the pay2send network to provide a payment method for electronic submission of documents to a government entity such as the united states patent and trademark office.