Comment #: 40

From: David Rasch
Sent: Thursday, September 30, 2004 5:36 PM
To: Authentication Summit
Cc: Ryan Allis; Aaron Houghton
Subject: Email Authentication Summit—Comments, (Matter Number P044411)

Email Authentication Summit—Comments, (Matter Number P044411)

IntelliContact Pro (by Broadwick Corporation) leads in the group of permission-based email marketing software providers for the small and medium sized business sector. We provide services to over 800 customers and send over 10 million permission-based emails each month on their behalf. These emails reach customers, prospects, and subscribers who have requested to receive the content in each email. These emails consist of newsletters, product offerings, and announcements from both for-profit and non-profit organizations. Through these emails, businesses keep in touch with their customers, inform them about changes in the business, and obtain repeat sales. Broadwick is well qualified to participate in the Summit in terms of knowledge and we will represent the interests of both email marketers and businesses using free software to provide email services.

Users of IntelliContact agree to a strict anti-spam policy. Our staff and design team make every effort to prevent our customers from sending spam and have no hesitation in terminating the accounts of suspicious customers or those who receive complaints. We respond to individual complaints of unsolicited messages promptly and personally to ensure this integrity. Any email lists which have been purchased, borrowed, rented, or obtained through sources other than direct individual permission are strictly prohibited for use within the IntelliContact Pro system.

We fully support the introduction of email authentication methods as a standard by which spam can be reduced or tracked at the very least. At a higher level, we support finding an alternative to the existing blacklist-based method. Currently, IntelliContact emails include full legitimate header information and each contain a valid and working unsubscribe opt-out link to ensure that users receive no further messages after they've requested to cease their agreement. As mentioned above, a method for opting-out does not supplant the responsibility for ensuring that the original lists of contacts have granted their permission to receive marketing emails.

We predicate our support for these authentication methods upon the feasibility of implementing these frameworks while continuing to provide an affordable email marketing service to our customers. Specifically, some proposed methods of sender authentication require more sender overhead, such as the DomainKeys proposal, which would be cost prohibitive to our company and our customers who wish to continue to use email to contact persons who have given their permission to be reached via email.

In addition, our business and product are built on and run with the assistance of free software, and any method of email authentication which cannot be fully implemented/adopted by free (open source) software will increase our costs and infringe upon the software licenses we currently utilize. The servers which send our emails all run the Debian/Linux operating-system which contributes to our success by keeping costs low and ensuring future scalability. By using commodity hardware and open source software our system scales up to many users without requiring the purchase of additional software licenses. In addition, we maintain the ability to customize and

tune our mail servers to deliver mail quickly, efficiently, and maintain our high rate of deliverability. Currently, the Debian/Linux team has announced they will be unable to include Sender ID technology due to its restrictive license.1 This is one of our main concerns with the proposal as it stands.

Efficacy

The proposed authentication methods will serve the purpose of reducing spam by increasing the cost of sending unsolicited email. Specifically, the use of sender authentication would cut down on the number of open-proxies and open-relays which can be used to send spam. Currently the process begins once a spammer obtains access to an open-relay or open-proxy. The spammer need only begin sending a stream of emails to this server to send his/her spam messages. By authenticating senders the spammer would need to have a registered domain (they couldn't use free Hotmail, yahoo, or other commodity accounts) and add the open server as a permitted sender for their domain. Not only does this create a higher barrier to the start of sending unsolicited messages, but it adds to the amount of forensic information collected, which assists in locating the individual who sent the message. We support the thrust of these measures.

However, due to the reasons listed in Licensing, a lack of universal support will hinder the proposed standards. Specifically, if major vendors and major software providers are unable or unwilling to include support, then very few providers will use sender authentication and in result, very few messages will have the necessary information to determine whether or not they are authenticated.

Coexistence/Backward Compatibility

A good proposal will be entirely backward and cross compatible. That is, the new technology will not completely prevent mail from being delivered or prevent delivery of non-compliant messages. However, the filters at the receiving end may be configured to filter non-compliant mail, or flag it as likely to be spam. The technologies can coexist on a single server, but there's a clear global advantage to implementing a unified standard for sender authentication rather than fighting spam on two separate fronts. Clearly, dividing the sender authentication into two separate frameworks will serve as a negative factor toward the level of adoption (more adopters yields higher probability that non-compliant messages are spam; see Licensing and Unauthenticated Emails for adoption problems).

Unauthenticated Emails

At this time and for the foreseeable future the unauthenticated status will contribute little if at all to an overall “score” obtained by a spam filter such as SpamAssassin. Due to the negligible domains with deployed sender authentication, dropping mail from unauthenticated senders would vastly increase the false-positive rate of any mail server. If a message were authenticated as “valid” then the “score” would probably be considerably reduced to reflect the trust established through the sender authentication. If an email arrived with support for sender authentication and the sender did not match the authorized senders it would be “invalid” and would thus receive a “score” indicating a much higher likelihood of spam.

The handling of unauthenticated email will become easier as the sender authentication schemes become widely deployed at that point; it will be highly probable that any unauthenticated email is spam.

False Positives and Negatives

Neither Sender ID nor DomainKeys are inherently vulnerable to either

false-negatives or false positives as they only detect whether the message came from a server which has been approved by the systems' administrator to send email on behalf of the domain. However, the users might send mail through their home ISPs, hotels, or other locations which don't automatically relay mail through their authorized mail servers. This will require administrators to make a more concerted effort to provide users on the road access to their mail transmission capabilities. In addition, ISP's will no longer be responsible for providing mail relay services for all of their customers not using the ISP's provided mailboxes.

Open Standard

Clearly a good scheme needs to be based on an open standard. Mail servers and clients currently run on many operating systems, platforms, and handheld devices. If the authentication standards were not open, then they would exclude some part of this population and thus make mail between these populations unauthenticated or impossible (not for the proposed schemes, but perhaps for others; see Coexistence/Backward Compatibility).

Licensing and Patented/Proprietary

Given the current license of the Sender ID standard and the declarations made by several major open-source software players it seems as though the scope of the deployment of the Sender ID technology will be severely hindered by conflicting and unacceptable licenses. The Debian project2 and the Apache Foundation3 have professed that they cannot implement Sender ID due to licensing incompatibilities. Other groups including the authors of a module for Sendmail to implement Sender ID have refused to sign the license and believe they aren't required to do so.4 Sendmail's CEO, David Anderson, said "his company was not going to sign the license agreement. Moreover, the company's lawyers do not think that anyone needs to." As of April 2003 it was estimated that 38+% of mail servers run the Sendmail software which has no interest in signing this license agreement.5 The dispute over the license needs to be settled, and there should be no patents or licensing restrictions encumbering the greater users of the internet from implementing this technology. Sender ID is currently patented and licensed by Microsoft Corp.

Outsourced Email Services

In the case of outsourced email services (like our product IntelliContact Pro), the provider may have to distinguish between the "Reply-to:" address and the "From:" address. The sender will have to be assigned a forwarding mail entry on the providers service. For example customer-a@intellicontact.com.

Computational Complexity and Scalability

The DomainKeys initiative has significant computational complexity as compared with the Sender ID framework. Cryptographically signing a message as originating from a given domain will add significant computational cost to delivering all email messages. This will adversely affect the cost-effective permission-based email marketing we provide to our customers by decreasing the amount of messages each server may send to the number which it can cryptographically process rather than the number of connections it can handle. The senders of permission-based email would have to bear this increased cost, a shame for the companies that are in fact abiding by the rules and even practicing good etiquette by sending only requested emails.

Primary Concerns

As a permission-based email marketing company, our primary concerns deal with

Computational Complexity, Scalability and Licensing. We're highly interested in reducing the affect of sender authentication on our product and its costs.

--
David Rasch
Broadwick Corporation (http://www.broadwick.com)
makers of IntelliContact Pro (http://www.intellicontact.com)
Sales and Support - (919) 968-3996