Comment #: 34

ColdSpark

Email Authentication Summit

Comments - Matter Number P044411

Contact:
Kelly Wanser
CEO, ColdSpark
kelly@coldspark.com
303-410-0751

This document and the information contained herein are confidential and remain the exclusive property of ColdSpark, LLC.

Position Statement

To address the problems in email networking arising from the lack of adqeuate methods to authenticate the origins of email messages against their purported source, including some types of spam and many types of illegal email, ColdSpark endorses an open authentication protocol for email that combines the methods proposed in the DomainKeys standards with an extension for the optional replacement of DNS key registries with separate key registration servers as proposed in the Identified Internet Mail (IIM) protocol. These protocols are sufficiently similar that it should be possible to rationalize their central method (key encryption and resolution) while supporting the key registration server method proposed in IIM as an extension to the main protocol.

Summary

ColdSpark supports the institution of an open authentication protocol for email, designed for widespread adoption by all Internet mail network operators and generally supported by existing technology and network infrastructure, to combat problems in email communications that are addressable by an effective method of accurately identifying senders. These problems include: the use of zombies and open proxies for illictly sending mail, "drive-by" spamming (i.e. sending spam from within another party's network without authorization), many common and effective methods of "phishing" and many common and effective methods of evading investigation and identification while engaging in illegal emailing and ecommerce practices.

While the SPF protocol, and its successor SenderID, provide some useful capabilities for authenticating the purported origin of a message against the domain at which it originated, this category of authentication method suffers from both a less robust or less "tamper-proof" process than other proposed methods and also is encumbered by proprietary intellectual property claims that place undesirable, and possibly impracticable, encumbrances on users.

The DomainKeys method for authentication decreases the ease with which illicit mailers can find and deploy methods to fool the authentication system, thus improving its effectiveness. Pending the finalization of its licensing method, it may also be more likely to be made available under a license scheme that is generally compatible with open source use. But, DomainKeys shares some of the deficiencies of SPF and other domain authentication protocols in introducing difficulties for network operators who would use authorized 3rd parties to send mail, or use email relays for a variety of legitimate purposes. It also lacks a more granular approach for authentication individual users,or subnets of users, within networks.

A seemingly effective approach to addressing these deficiencies is contained in the Identified Internet Mail protocol, which shares the DomainKeys method of using key encryption derived from individual message components for authentication, but introduces the use of a separate key registration server, as opposed to additions to the DNS server, to host key information. This advance reduces the complexity of actions performed by the DNS server and adds the ability to host keys, and thus authenticatte messages, by individual senders or groups of sender on the networks. This produces a number of advantages for the operators of large networks and hosting systems and also for the networks that receive messages from them.

ColdSpark endorses an open authentication protocol for email that combines the methods proposed in the DomainKeys standards with an extension for the optional replacement of DNS key registries with separate key registration servers, as proposed in the Identified Internet Mail (IIM) protocol. These protocols are sufficiently similar that it should be possible to rationalize their central method (key encryption and resolution) while supporting the key registration server method proposed in IIM as an extension to the main protocol.

Problems Addressed By Authentication Protocols For Email

Based on ColdSpark's research and analysis of traffic consisting of billions of messages passing through email servers in the networks of our customers, ColdSpark has found that "undesirable" or "illegitimate" email can be classified a number of ways, some referencing the preferences of the recipient and others referring to the origins of the messages. The term "spam" is often used with respect to the former, and classified subjectively.

For network operators, however, determining the origin of emails has become central to techniques used to reduce the amount of undesirable email, as different methods of generation are used more frequently by "spammers" and, for those engaged in the most illegal or illicit practices, masking the origin of the messages, and therefore the identity of the sender, are an important part of evading the consequences of their practices.

As a consequence, successful methods for accurately authentication the origin of an email against its purported source will have a dramatic impact on certain practices within the total universe of spam and other problematic mail traffic. These include: worm traffic, zombies, open proxy mailing, "drive-by" spamming and many forms of phishing and spoofing.

No authentication protocol will adequately address all forms of spam, particularly as it is defined subjectively. It is ColdSpark's view that an effective authentication protocol is likely to make a significant reduction in the total share of spam as a portion of all mail traffic, and significantly impair the operations of the most egregious and fraudulent spammers.

We estimate that the right protocol, with reasonably wide adoption among major network operators, will reduce gateway spam, worm and other problematic traffic by 30% or more, representing not a perfect solution to the problem of spam as perceived by users (and practiced by the operators of ISPs, mail hosts and "permissioned" services), but a powerful tool for network operators to eliminate harmful, high-volume traffic at or near the network gateway, with little risk of false positives.

General Considerations

Email/SMTP is one of the most successful open protocols used on the Internet, and has facilitated the transition of communications from more labor intensive, time consuming media to an instantaneous, inexpensive electronic channel. One of the critical success factors for email, as for other Internet protocols, is its open standards and the widespread availability of free, open-source applications for its deployment. In addition, email requires no centralized repository of information, or central network facility. Email is a non-centralized, standards-based protocol enabled for use by anyone with limited computer hardware and access to a myriad of open-source or commercial applications and tools.

For an authentication protocol to be useful for email, it must be widely used, and, therefore, must be readily implemented with consideration for existing hardware, software and network environments and existing levels of expertise and resources. Given the history of email, and the customary practices of its network operators, it must also be compatible with open source usage and not strictly embodied as a proprietary product or strictly enabled through a proprietary service.

In order to succeed, this recommended protocol MUST be:

- Available for use under a license that is compatible with open source practices, including sublicensing by commercial companies
- Compatible with today's MTAs and the hardware they commonly operate on

It is also imperative that no single commercial entity own, maintain control of or responsibility for any aspect of the solution. Under no circumstances should a solution imply a marginal payment, subscription fee or membership to any service. Nor should any solution require a change to the base SMTP protocol or disable the operation of email for servers that do not immediately employ the solution.

It should, in so far as possible, maintain the same open source, non-centralized, free use that is practiced today with the existing generation of email applications and protocols.

Proposed Methods

SPF and *SenderID*

The SPF protocol, and its successor SenderID, provide some useful capabilities for authenticating the purported origin of a message against the domain at which it originated. The core method for SPF uses a look-up to match the sender as identified by the From address in the envelope of the message communicated ot the receiving server during the SMTP commincation (not in the header of the message) with an SPF registry posted as an augnmented listing in the DNS (Domain Name Server).

Sender ID proposes to improve this method by replacing the look-up using the envelope from address with the use of an algorithm that analysis header information to derive the “Purported Responsible Sender” (PRS) and is therefore more likely to be able to identify efforts to mislead message recipients by displaying alternate *From* addresses.

Both methods suffer from potential workarounds by illicit mailers. SPF itself fails to address the situation of correctly matched SPF look-ups that nonetheless communicate false information to recipients. SenderID closes gaps on this problem but leaves openings for efforts to fool the PRS algorithm, which is also the most proprietary part of the SenderID standard.

DomainKeys

DomainKeys offers a much more bullet-proof method for ensuring that identities cannot be falsified by replacing the process of looking up *envelope from* or PRS with the generation of a unique encrypted key for each message that is matched to a public key made availble through an expanded registration on the DNS server. This method better protects against efforts to spoof the system and, as a by product, ensures that messages cannot be tampered with or altered enroute, as such tampering would alter their keys and disable their decryption.

While this represents an improvement, it creates new challenges for newtork operators and others who use 3rd parties to send email - and thus would not post keys on the same DNS registries - or who use more complex relays in their mail networks (e.g. global enterprise mail networks). For these types of operators, there would be an advantage to providing more flexiblity and granular control over the posting of key registries.

Identified Internet Mail (IIM)

Identified Internet Mail leverages the principle mechanisms of DomainKeys, key encryption for indidiviual messages with registry look-ups via DNS actions, but adds granularity, flexibility and control by using the DNS look-up to point to a separate Key Registry Server (KRS) that can host lists of individual senders and sender groups within a network, each with their own keys. This supports authentication down to the user-level, assignment of email authentication to 3rd parties and flexible configuration of email and DNS servers for the operators of large networks through control of their interfaces with the KRS.

Proposed Solution:
DomainKeys and Identified Internet Mail (IIM) Combined Protocol

It is ColdSpark's view that a solution that combines the features of DomainKeys and Identified Internet Mail into a single protocol that supports both "domain-level" implementation via DNS registries and "granular" implementation for user-level authentication and more flexible network options for large network operators.

Such a solution could be readily adopted by most network operators without major changes to their infrastructures or systems; would automatically provide an instant improvement in authentication with widespread use of an effective domain-level method; would accommodate the requirements of large networks, 3rd party operations, mail forwarding services and unusual architectures; and would provide a frictionless pathway for the adoption of advanced, user-based authentication as adoption grows.

As a server-based protocol that leverages the action of the existing MTA and DNS, such a system should be transparent to end-users, readily scalable and fully compatible with the current open, private, unencumbered use of email.

Adoption

Provided an effective protocol is made available under acceptable licensing terms, adoption may be rapid, particularly if led by major ISPs. ColdSpark believes that the rate of adoption and the efficacy of the solution are likely to follow the trajectory of reverse DNS for email. Initially, the method was used to identify and prioritize email that could be deemed to be more "legitimate" and, as use became more widespread, the method is increasingly a minimum requirement for all messages.

It should be noted that encryption-based solutions add processing to email activities, most of the burden of which is placed on the receiving network. It is our view that this processiong can be minimized, and should not have an inordinately burdonsome impact on receiving networks. Most importantly, this burden should be far outweighed by the reduction in problematic mail traffic and, as borne by ISPs, compliants from customers arising from spam, phishing and email fraud.

About ColdSpark

ColdSpark is the leading provider of email infrasctructure solutions to Global 2000 companies and large internet network operators. Dedicated to the wholesale upgrade of today's legacy mail network systems, ColdSpark has created the next-generation of email delivery with the patent-pending SparkEngine, the world's most powerful mail transport agent (MTA) with its unique open API framework for flexible interoperation with any existing systems, emerging protocols and/or custom applications and scripts. The SparkEngine is the foundation of ColdSpark's suite of sophisticated email security, policy management and marketing automation applications. ColdSpark offers enterprises and services providers the most powerful, flexible, secure and cost-effective email networking solutions available.

Founded in 2000 by email technology veterans, ColdSpark's customers include Lehman Brothers, AT&T, Equifax, Comcast Cable and Media News Group. For more information on ColdSpark's products and services, visit: http://www.coldspark.com.