Internet Messaging Leaders Work Together to Fight Email Fraud

Email Testing Event Strengthens Sender Accountability

DALLAS, Texas and SUNNYVALE, California – November 6, 2007 – In the ongoing battle to combat **email fraud** and **phishing scams** that diminish the value of legitimate email, a group of dedicated engineers from 20 leading ISPs, messaging product companies and industry associations gathered for two days to test **DomainKeys Identified Mail (DKIM) – an email authentication standard** recently approved by the **Internet Engineering Task Force (IETF)**. DKIM permits an organization to add a digital "fingerprint" to outgoing email. Receivers can then validate the message using the organization's domain name, such as "example.com".

Testing covered different scenarios for signing and validating email messages between participants' products and services. Progress was tracked on a large matrix, which recorded each successful interoperability test. By the conclusion of the event, the matrix was nearly 100% complete!

"Because **spam and phishing** continue to proliferate, messaging companies are eager to move forward with wide-spread **implementation of DKIM**, to help consumers and businesses identify legitimate email messages," said Dave Crocker, principal of Brandenburg InternetWorking, a Sunnyvale, California consultancy, and one of the event's coordinators. "This much progress for a new standard's first testing event is extremely unusual. We have demonstrated that DKIM is easy to add to an **email service** and that its use of **cryptographic technology** provides a strong basis for knowing received email really is associated with the organization that claims to have sent it. "

"We learned a lot by participating; not the least of which is that DKIM just works," said Arvel Hathcock, Founder and CEO of Alt-N Technologies, and host of the event. "The testing performed by all participants revealed no significant barriers to adoption or use."

DKIM uses domain names, rather than the more cryptic IP Address numbers, to represent an organization's identity, because domain names are more stable and are already used to identify organizations on the Internet. The standard allows email senders to insert a cryptographic signature or "fingerprint," which only they can create. This signature travels within the message itself, allowing authentication to take place without regard to the path the message follows to reach a recipient. When the signature is later validated, a recipient can be assured of the signer's identity and that the message was not tampered with during transit over the Internet.

A valid DKIM signature provides reliable input for **domain-based reputation** assessment. Incorporating the standard into messaging products provides an additional layer of email trust and protection to receivers concerned with threats of email fraud and phishing scams. DKIM also arms senders with a stronger means of brand protection.

Engineers traveled from locations as far away as France and Japan to attend the Dallas, Texas event. The twenty participating companies and organizations were: Alt-N Technologies, AOL, AT&T Inc., Bizanga Ltd., Brandenburg InternetWorking, Brandmail Solutions, ColdSpark, Constant Contact, Inc., DKIMproxy, Domain Assurance Council, Google Inc., ICONIX Inc., Internet Initiative Japan (IIJ), Ironport Systems, Message Systems, Port25 Solutions, Postfix, Sendmail, Inc., StrongMail Systems, and Yahoo! Inc.

.

About Alt-N Technologies

Alt-N Technologies delivers innovative, affordable and secure messaging and collaboration solutions that are used by businesses in over 90 countries and 20 languages worldwide. Headquartered in Grapevine, Texas, Alt- N Technologies' flagship solution, the MDaemon® email server, provides a standards-compliant, feature-rich platform that is virtually virus and spam free and is quickly and easily installed and managed. For more information, visit ***www.altn.com****.*

About Brandenburg InternetWorking

Brandenburg InternetWorking assists clients in developing network-based applications businesses, designing system architectures for them, and pursuing industry standardization as a strategic corporate effort. Brandenburg offers thirty-five years of expertise, developing distributed information system products, services and businesses. For more information, visit ***www.bbiw.net****.*

Additional information about DKIM can be found at ***www.dkim.org****.*