RFC5451bis

Authentication-Results Header Field Update

Murray S. Kucherawy
<msk@cloudmark.com>
What It Is

• From 2000 forward, there was a number of efforts to create message sender authentication mechanisms
  – SPF (RFC4406), Sender-ID (RFC4407-8), DomainKeys (RFC4870), DKIM (RFC4871) all appeared during this period
• Each of these created a header field for the purpose of relaying the receiver-side results of authentication efforts
  – Different field names, different formats
  – Lots of separate parsing code, lots of room for mistakes
What It Is

• RFC5451 defined a new message header field called Authentication-Results that provides a common location and format to collect this data

• Also describes under what conditions the field should be added by verifiers, and when it should be ignored or removed for trust reasons
Deployment Experience

• Lots of deployment has been observed since publication
  – Open source MTA plugins: OpenDKIM, dkim-milter, dk-milter, sid-milter, hashcash milter
  – Open source webmail: Roundcube
  – Other open source: DKIMproxy
  – Commercial: Gmail, Yahoo!, AOL (someday)
Deployment Experience

• A few issues have come to light that the original didn’t address
  – Original specification has no way to indicate, for a message with multiple DKIM signatures, which signature’s result is being reported
  – There is demand for a mechanism to indicate proxied results, such as the result of verification a list manager did prior to altering the message
RFC5451bis Effort

• Work is beginning on an update draft to address these two industry needs
• Will be offering it to the DKIM Working Group (SEC) first since both issues relate particularly to them
• If they aren’t interested, will seek individual submission sponsorship from APPS again
• Probably doesn’t need a WG of its own, but we can go that way if needed
RFC5451bis Effort

• Beginning to gather interested parties to restart the discussion given the new ideas
• Mailing list (mail-vet-discuss@mipassoc.org) is still available
  – Will post the current draft there soon to get things going, as well as to the I-D repository
• Will also post to DKIM WG list to see if they want to take up the work
  – Somewhat related to one of their re-chartering items
• Interested parties welcome to join