DKIM Sender Signing Practices
December 2007 Update

Jim Fenton <fenton@cisco.com>

What's new?

- New (-01) draft published September 17
- New "handling" tag added

  Expresses preference about handling of Suspicious messages
- Removed discussion on "Third party Signatures and Mailing Lists"

  Better covered in Overview Document
- Clarified record syntax

  Records with unknown tags are syntactically correct
- Numerous wording improvements

SSP “Handling” Tag

- New SSP tag added in -01 in response to user community requests
- Two values:

  “process” (default): process Suspicious messages

  “deny”: Alleged Originator requests that Suspicious messages not be delivered
- Use case: Domains that emphasize security over deliverability
- Adherence to “deny” is optional on the part of the verifier

  It’s a request from the SSP publisher

"DKIM has allowed the largest targets of online fraud and phishing, the financial services industry, to begin positively asserting e-mail that is legitimately from them. Conversely, we are looking toward SSP as a way to apply strong policy regarding e-mail that falsely purports to be from one of our domains. In other words, this policy framework needs to provide a clear intent related to the assertion of the sending institution, including a strong capacity for dealing with unsigned mail or malformed signatures, including the intent for this type of message to not be delivered to the customer mailbox."

Erik Johnson
Bank of America

"Delivering an email that has failed a DKIM check as "Suspicious" may fit most use cases but not all. Domains that are targeted for Phishing need a mechanism of informing recipient domains that they have "no confidence" in unsigned or improperly signed email. These emails should be treated as potential threats and NOT delivered to the Intended recipients. A SSP "Deny" option would provide the ability for domains that fit this use case to recommend rejecting or quarantining email that has failed DKIM verification."

Jeff Carnahan
US Bank

SSP Open Issues

Issue	Title Submitter	Age
1382	(SSP) New Resource Record Type Scott Kitterman	1 year ago
1399	Clarify i= vs. SSP Mike Thomas	1 year ago
1402	Applicability of SSP to subdomains Jim Fenton	12 months ago
1512	SSP should not link “all” and third parties Mike Thomas	4 weeks ago
1513	The new handling tag Mike Thomas	4 weeks ago

#1382: New Resource Record Type

- “Recommend a new requirement that the protocol MUST NOT depend solely on a new DNS RR type”
- Current draft does not use a new RR type at all
- Suggest Closing

#1399: Clarify i= vs. SSP

- "…need to provide the exact semantics in SSP of how a receiver determines whether a DKIM signature satisfies the SSP criteria or not."
- Think it's clear now:

  All -> any signature that verifier wants to accept

  Strict -> Signature that i= matches From: address

- Close this?

#1402: Applicability of SSP to Subdomains

- Should SSP “bleed through” to subdomains to avoid the use of unexpected subdomains/hosts to avoid SSP?
- Current draft allows 1 level of downward applicability for SSP records unless “s” is set
- Multiple levels require explicit SSP publication
- Reasonable compromise? Close?

#1512: SSP should not link “all” and third parties

- “…inappropriately links the existence of a third party signature to the “all” signing practice”
- Draft is worded awkwardly: Verifier Acceptable Third-Party Signatures MUST…
- “Third-party” concept may be unclear
- Perhaps remove third-party signature concept, and simply say that domain may consider message not Suspicious if there is any signature it wants to accept
- No discussion of this on the list yet. Thoughts?

#1513: the new handling tag

- "…the new handling tag is probably not needed…it should perhaps be a non-normative discussion in 'All' and 'strict'."
- Is there a need for combinations like All/Deny and Strict/Process?
- Or should Deny/Process be (perhaps non-normative) side effects of Strict/All?
- Little discussion so far. Thoughts?

New issue: Responsibility vs. Validity

- DKIM-base defines a signature as “taking responsibility” for a message
- Does not make any assertion of correctness of From: header field, yet SSP checks for a binding
- Proposal: Publishers of SSP (other than Unknown) MUST ensure that when the signing and From address match, that the From address is “valid” (authorized)

New issue: Granularity of comparison

- Should the comparison of Signing Address against the From: address consider the local part?
- Argument against:

  Signing address (and g= in key) could use an arbitrary tag in place of a “real” address in the local-part

  DKIM is a domain-level mechanism
- Argument for:

  Intent of constraining signing address with g= is to ease key delegation by not giving authority to sign for the entire domain

  Need to check local-part in order to make SSP consistent with base (not void the g= mechanism in base)

  There are many other places for arbitrary tags, if desired

Next Steps

- Issue -02 draft with feedback from this meeting
  - In a week or so
- Write comparison with related documents
  - RFC 4686 (DKIM Threat Analysis)
  - RFC 5016 (SSP Requirements)
- Working Group Last Call mid-Dec -> mid-Jan