Third-Party DKIM Policy IETF 70

Transparent and Flexible Policy Compliance

Douglas Otis

Doug_Otis@trendmicro.com

http://www.ietf.org/internet-drafts/draft-otis-dkim-tpa-ssp-02.txt

SSP is based only upon the From header

SSP assertions disqualify From headers NOT signed by the same or parent domain, or NOT encompassed by the i= parameter. (i= parameter disqualifies signatures generated by g= restricted keys not matching the From header.)

The All and Strict assertions allow:

- Detection of disqualified From headers (All)
- Rejection of disqualified From headers (Strict)

SSP All/Strict might be suitable for transactional messages, but are not suitable for normal use. The i= requirement prevents Sender and Resent-* headers from being unambiguously signed.

Why TPA-SSP policy extensions?

- TPA-Labels Authorize Third-Party domains and provide:
  - Minimized Administrative complexity
  - Autonomous Authorizations
  - Separate policy assertions regarding header/i= scopes
  - Elimination of DNS delegation or Key exchanges
- Scope parameters provide:
  - Means to minimize TPA related overhead
  - Means to limit qualified headers without constraining i=
  - Means to indicate whether the i= validates:
    - the identity associated with email-address
    - the account submitting message

TPA checks made when otherwise disqualified

- The message is Qualified when:
  - From SSP Scope= O with a valid signature for Sender or Resent-*
    (eliminates i= parameter conflicts)
  - From SSP Scope= A with a valid signature
    (eliminates i= parameter conflicts)
  - From SSP Scope wo/NO-TPA & TPA-SSP in From domain for a valid signature d=
- Identity/Access assertions are in TPA-SSP

Sub-Domains are Third-Party Signers

- A sub-domain will NOT provide valid DKIM signatures for SSP From header All or Strict
- Proliferation of email sub-domains weaken recognition of well-known domains
- Without TPA-SSP, well-known domains are unable to assert more than one policy
- Authorized third-party domains allow different policy inheritance

Originating Headers defined in Scope

From == Author(s)

Sender == Agent for Author

Resent-* == Agent reintroducing message

SSP / TPA-SSP scope:

- F (From), O (Sender or Resent-*)
  (policy compliance scope for acceptance)

- M (MAILFROM)
  (signatures authorized for DSNs)

Granularity within Domain Signatures

- Scope (-i) suffix

  Asserts unambiguously signed identity is authenticated

- Scope of A/<hours>

  Asserts the identity included within the DKIM signature uniquely tracks accounts granted access over the specified number of hours

(Large domains are increasing being exploited by bots. Abuse is doubling every 6 months.)

Advantages for TPA-SSP

- Allows greater policy flexibility
- Simplifies administration of third-party authorizations
- Permits autonomous third-party authorizations
- Eliminates need for sub-domain email-addresses
- Transparent policy/signing domain differentiation
- Eliminates DNS domain delegation or Key exchanges
- Reduces email breakage
- Clarifies meaning of i= signature parameter
- Clarifies when reputation can be applied to identities
- Traces who introduced the message