allman-dkim-ssp-02

Jim Fenton <fenton@cisco.com>

IETF 68 – Prague

March 21, 2007

SSP recent changes

- Removal of “user” policy
- Change in tag names to promote extensibility

  p -> dkim

  t -> dkimflag
- Changes in SSP algorithm to fix problem described at last IETF
- Current draft is expired, but new one coming soon!

SSP Open Issues

- New “DKIMP” resource record vs TXT record
- “Strict” policy
- Policies placing limitations on selectors
- Policies on multiple signatures to aid algorithm transitions
- Use of PTR/XPTR to locate record
- Resolution of open issues on SSP requirements

New SSP Algorithm (1 of 2)

- 1. If a valid Originator Signature exists, the message is non-Suspicious, and the algorithm terminates.
- 2. Query DNS for a DKIMP record corresponding to the domain part of the Originator Address. If the result of this query is a NODATA response, proceed to step 6. If the result of this query is a NXDOMAIN response, the message is Suspicious and the algorithm terminates. Otherwise, proceed to the following steps using the record retrieved by the query.
- 3. If the SSP "dkimflag" tag exists and any of the flags is "t" (indicating testing), the message is non-Suspicious and the algorithm terminates.
- 4. If the value of the SSP "dkim" tag is "unknown", the message is non-Suspicious and the algorithm terminates.
- 5. If the value of the SSP "dkim" tag is "all", and one or more Valid Signatures are present on the message, the message is non-Suspicious and the algorithm terminates. Otherwise, the message is Suspicious and the algorithm terminates.

New SSP Algorithm (2 of 2)

- 6. (check for parent domain policy) If the parent domain of the previous query is a top-level domain (e.g., a country code) or is on a list of invalid signing entries maintained by the verifier (see dkim-base section 6.1.1), then an SSP record was not found and the message is non-Suspicious and the algorithm terminates.
- 7. Query DNS for a DKIMP record corresponding to the immediate parent of the previous query. If the result of this query is a NODATA response, then proceed to stop 7.
- 8. If the SSP "dkimflag" tag exists and any of the flags is "t" (indicating testing) or "s" (indicating that the record should not be used apply to a subdomain), the message is non-Suspicious and the algorithm terminates. Otherwise proceed to step 4.

New SSP algorithm - comments

- We’re back to an upward search, but only when a wildcard is present
  - Wildcards *seem* to be relatively rare
- Alternative would be to publish wildcard SSP
  - Would also need to publish a “shadow” SSP record for every defined name in the zone
  - Puts more burden on the publisher

Algorithm with TXT records

- TXT records would use a prefix, e.g., _policy
- NXDOMAIN on a query only means there’s no policy
    - Separate query needed to see whether the domain exists
    - Could be overlapped with policy query
- Tradeoff of lookups vs. ease of deployment of TXT records