allman-dkim-ssp-02

Jim Fenton <fenton@cisco.com>

IETF 67 – San Diego, California

November 7, 2006

Major Changes Since -01

- Now called “Sender Signing Practices”
- Records now published using a “custom” DNS RR
- Changes in the record search algorithm
  - Fewer upward searches
  - But there are bugs – more later on this
- Syntax changes: More human-friendly, less SPF-like
  - But slightly longer
- Minor changes to user-level behavior

Why a New RR Type?

- Observation: Want to know if the domain exists

  If you detect a non-existent domain, it isn't necessary to query parent domains

- Searching for a TXT record with a prefix doesn't tell whether the domain exists or not

  NXDOMAIN from query for _policy._domainkey.example.com TXT record says the SSP record doesn't exist, but says nothing about example.com's existence

- Searching for a DKIMP record MAY tell you this

  NXDOMAIN from query for example.com DKIMP record says the domain doesn't exist, therefore the message is Suspicious

  But NODATA is still returned if a record of another type exists, or if there is a wildcard in a parent domain

The Algorithm

- Section 4.3 of the draft
- 13 steps -- looks a little daunting -- but it isn’t really

  Took a very pedantic approach to describing it, for clarity

- The bug: Assumption that non-existent labels can be identified through NXDOMAIN response

  Wildcard records cause this to fail, not just for one hierarchy level, but at all levels

  For example, can’t detect a.b.c.d.e.f.g.sun.com because *.sun.com MX record exists

- Solution: More upward search is required, but NXDOMAINs, when received, still terminate the search

User-level Signing Practices

- User-level signing practices are now a separate flag from domain signing practices
  - Domain record can now express default practices
  - User-level practices override domain when present
- Effect: No longer necessary to publish user-level records for all addresses in a domain
- Need (or lack thereof) for user-level practices is still an open question

Requirements - Discovery

Req #	Description	Y/N	Comment
6.1-1	Publication subordinate to author's domain name	Y	Published in new DNS RR in alleged author's domain
6.1-2	Definitive response within a small, deterministic number of queries	Y	Draft uses 2 queries but has problems when wildcards exist; can limit to 5 as in previous draft
6.1-3	Unambiguous semantics WRT other uses of publication mechanism	Y	Newly-defined RR type is unused by any other mechanism

* Provisional Requirement

Key:		
	🟩	Compliant
	🟨	Non-Compliant - Provisional
	🟥	Non-Compliant

Requirements - Transport

Req #	Description	Y/N	Comment
6.2-1	Widespread deployment of transport layer	Y	UDP (DNS)
6.2-2	Low cost: low latency and packet count	Y	DNS: designed for low cost
6.2-3	Caching semantics defined if not already existing	N/A	Leverages DNS caching
6.2-4	Multiple geographically and topologically diverse servers	Y	Provided by DNS

* Provisional Requirement

Key:
🟩 Compliant
🟨 Non-Compliant - Provisional
🟥 Non-Compliant

Requirements – Practice/Expectation

Req #	Description	Y/N	Comment
6.3-1	Practices and expectation assertions about DKIM use: 2822.From address	Y	
6.3-2*	Assertion that domain doesn’t send mail	N	
6.3-3	“Null” practice	Y	“p=unknown”
6.3-4	“DKIM Signing Complete” practice	Y	“p=all”
6.3-5	Expectation of verifiable first-party signature	Y	“p=strict”

* Provisional Requirement

Key:
🟩 Compliant
🟨 Non-Compliant - Provisional
🟥 Non-Compliant

Requirements – Practice/Expectation

Req #	Description	Y/N	Comment
6.3-6	Intuitive descriptors		Unknown, all, strict, yes, no, t, s
6.3-7	No designation of other signers	Y	
6.3-8*	Ability to key off local part of address	Y	"u=yes" and subsequent query
6.3-9	No mandate of disposition by receiver	Y	
6.3-10	No publication of disallowed third-party signers	Y	

* Provisional Requirement

Key:

🟩	Compliant
🟨	Non-Compliant - Provisional
🟥	Non-Compliant

Requirements – Practice/Expectation

Req #	Description	Y/N	Comment
6.3-11	Evaluation not required if valid first-party signature	Y	Section 4.3 step 1
6.3-12*	Practice enumerating acceptable crypto algorithms	N	Conflicts with 6.3-11; already specified in key records
6.3-13	Do not impugn the existence of first-party signatures	Y	

* Provisional Requirement

Key:
- 🟩 Compliant
- 🟨 Non-Compliant - Provisional
- 🟥 Non-Compliant

Requirements – Extensibility

Req #	Description	Y/N	Comment
6.4-1	Evaluation not required if valid first-party signature	Y	Section 4.3 step 1
6.4-2	Practice enumerating acceptable crypto algorithms	N	Conflicts with 6.3-11; already specified in key records

* Provisional Requirement

Key:
🟩 Compliant
🟨 Non-Compliant - Provisional
🟥 Non-Compliant