Author
DKIM ~~Sender~~ Signing Practices
March 2008 Update

Jim Fenton <fenton@cisco.com>

What (else) is new?

- New (-03) draft published February 23

- Major restructuring compared with -ssp-01:

    No more "suspicious": just output the practices

    Handling flag removed

    Practices now {Unknown, All, Discardable}

    Silent on "third-party" (non-Author) signatures

    Consistent treatment of multiple Author case

- Many wording changes

    More clear that recipients do what they want

How did we get here?

- "Inspired" by mailing list discussion on -ssp-01, Eric Allman (primarily) worked on a much simplified SSP draft

- In parallel, a group led by John Levine did the same

- I sent a "teaser" message to the list to gauge interest in the simplified draft

- John contacted me regarding the parallel effort, and we compared drafts

- The similarities were striking

- We smooshed them together, and you have -ssp-03.

ASP issues - Proposed Closure

Issue	Title	Comment
1399	clarify i= vs. SSP	Duplicate of 1519
1402	Applicability of SSP to subdomains	Duplicate of 1534
1512	ssp should not link "all" and third parties	-ssp-03 silent on 3rd-party sigs
1525	Restriction to posting by first Author	Changed in -ssp-03
1529	Change "originator" to "author"	Changed in -ssp-03
1530	replace use of term "suspicious"	Term not used in -ssp-03
1531	"does not exist"	Now "does not exist in DNS"
1532	Revise list labeling	List removed in -ssp-03
1533	Strict vs. integrated	Strict not used in -ssp-03
1535	Simplify SSP decision tree	Much simpler in -ssp-03
1536	Definition of action terms	"Reject", "bounce" not used
1537	Reputation is out of scope or define it	Reputation not mentioned
1538	Normative vocabulary usage	Extensively changed in -ssp-03
1540	Deprecate t=testing	t=testing eliminated
1550	Rename SSP to ASP	All but the filename have changed

ASP issues - Closable?

Issue(s)	Title	Comment
1382	New resource record type	Have we settled on TXT?
1513	The new handling tag	Is this about a separate handling tag, or giving handling guidance (1520)?
1521	Limit SSP to unsigned messages	
1522	Discussion of query traffic overhead	Maximum 3 queries. What else needs to be said?
1523	Service model summary	In overview document?
1524	Signature semantics	
1526	SSP applies to receive-side filtering, not end-users	
1527	SSP threats analysis needed	New text from Wietse added
1528	False negatives and positives	Predicated on use of "suspicious"?

ASP issues - Closable?

Issue(s)	Title	Comment
1541	Do we need SSP for DKIM=unknown?	Need: No. Nice to do (for lookup efficiency): Yes
1542	SSP restrictive policies recommendation for 4871 upd	
1543	Remove [FWS]	Variety of opinions on what we should allow: CRLF legal?
1547	MX Record Publishing Mandate	Strong list consensus against

ASP issues - Discussion needed!

Issue	Title	Comment
1519	Unnecessary constraint on i=	Domain or user granularity?
1520	Limiting ASP to statements that inform recipient about (potential) sender actions	Is Discardable OK? (see 1546)
1544	SSP version numbers	Do we need them? What are their semantics?
1545	Signed vs. unsigned header fields	
1546	Discardable inappropriately specifies possible verifier action	(see also 1520)
1548	Policies required to close security threats	
1549	Security threats are [not] well defined	
1551	Policy scope	Limit to SMTP?
1552	Threat: Unexpected third party senders	Similar issue to 1549?

User vs. domain granularity of ASP

- Opinion #1: DKIM is a domain-level signature, so ASP should also be at that granularity

    Concerns expressed about privacy concerns, etc.

    Desire to use i= local part as an opaque tag

- Opinion #2: DKIM is mostly domain-level, but keys can be delegated for specific signing addresses. ASP should reflect this.

The Discardable Practice

- Questions about the word "Discardable"

  Rough Consensus on a word seems difficult to achieve

  Do we need to go back to symbols? (hope not)

- Is Discardable (by whatever name) appropriate as a practice?

  Doesn't describe what the publisher of the practice does

  Lots of people think it's really useful

  It is only advisory