Introduction to SSP

Jim Fenton <fenton@cisco.com>

22 March 2006

SSP – The Name

- Originally “Sender Signing Policy”
- “Sender Signing Practices” probably a better name
    - Avoids over-use of the word “policy”
    - More descriptive and less prescriptive – this is the intent
- But SSP is really correlated with Originator Address
    - Should it be “Originator Signing Practices”?

SSP – The Intent

- Suppose a verifier gets an unsigned message from example.com
- It would be helpful to know whether example.com normally signs their mail
- If it does, and this message isn’t signed, it’s “suspicious”

Suspicious

- **Used to describe messages that aren’t consistent with an originator’s signing practices**
- **Intentionally vague – doesn’t say anything about what to do**
- **Some legitimate messages will likely be suspicious**
  - **Messages through lists that munge messages and don’t re-sign them**
- **It’s probably not good to over-react to suspicious messages**
  - **Deleting them outright, without considerable experience**

Originator Address

- The address in the From header field

  i.e., the author of the message [RFC 2822 3.6.2]

- Not the Purported Responsible Address

  Absent a valid signature, there is no purported responsibility, as far as DKIM is concerned

  This has nothing to do with IPR issues!

Third-Party Signatures

- Sometimes intermediaries modify message content
  - Mailing lists do this a lot
- Some applications “legitimately” spoof addresses
  - “Mail this article to a friend”
- Third-party signatures allow third parties such as these to take responsibility for the message
- Acceptance of arbitrary third-party signatures is arguably a huge security hole!

Finding the SSP

- SSP is found using the origination address in the message
- example.com SSP is located at _policy._domainkey.example.com
- SSP lookup is not needed if a valid origination address signature is found
  - SSP only offers information that is relevant in its absence

SSP Policies …er… Practices*

Symbol	Proposed Name	Meaning
~	NEUTRAL	Signs some mail
-	STRONG	Signs all mail
!	EXCLUSIVE	Signs all mail; third-party signatures should not be considered valid
.	NEVER	Entity never sends mail
^	USER	Repeat query at user level

* As of draft-allman-dkim-ssp-01

Some SSP issues

- Questions about cryptic “SPF-like” syntax
- Suggested additional practices:
  - “I don’t sign anything”
  - “I don’t sign everything, but don’t accept third-party sigs”
- Concerns about not consulting SSP if valid OA sig
- Reporting address (r=) tag
  - Localpart only (to avoid directing complaints elsewhere)?
  - Is a reporting address even appropriate?