Name Paths as Policies

DKIM IETF 66

Blocking spoofs & avoiding DoS

Douglas Otis

Doug_Otis@trendmicro.com

http://www.ietf.org/internet-drafts/draft-otis-smtp-name-path-00.txt

Forward Reference PTR RRs Defining Paths

- PTR RRset
  - Is forward referenced
  - Is isolated through unique underscore label
  - Provides name compression
  - Is not constrained by automated DNS services
  - Describes extensive email Name Paths
  - Offers greater extensibility without DoS risks
- Email Address Path allows >1000 packet amplification!
- Special host names define the nature of the path:

  “*.” == “Open-Ended”

  “.” == “Closed-Ended at Domain”

  “-.” == “No Path or No Service Offered”

Third-Party Signature Associations

Does OA email-address domain permit Third-Party Signers?

; not just ssp yes/no, but specific domains listed (open-ended)

_oasd._smtp.<email-domain>. PTR <dkim-domain-1>.
<dkim-domain-2>.
“*.”

; only email-domain allowed (close-ended)

_oasd._smtp.<email-domain>. PTR “.”

; email-domain offers no email service (shut)

_oasd._smtp.<email-domain>. PTR “-.”

Name Path Approach Helps Mitigate Denial Of Service & Replay Attacks

If OA != DKIM-domain
→ check signature requirement
_oasd._smtp.<dkim-domain> PTR required signing domains

Name Path can also compare against ancillary verified Reverse DNS or Client Host Name for a mitigation strategy.

If no OA/DKIM-domain or ancillary association
→ delay acceptance or white-list

Ancillary association can otherwise bypass this grey listing for a safer means for protecting verifier resources with fewer exceptions.

Conditional delay based upon Name Path association failure affords more effective third-party blocking.

Future Efforts for high impact SSP threats

- Annotation based upon trusted transactional domain lists
- Signing domain partitioning based upon signature parameters (will not require per user DNS RRs)

See http://www.ietf.org/internet-drafts/draft-otis-dkim-reliance-level-00.txt

In conclusion-

Signing policy, with either flags or name lists, will not prevent look-alike message abuse. With Name Paths, DoS solutions are also available while enjoying greater freedoms. Be prepared to respond with solutions addressing newer concerns that become significant with email-address internationalization and barriers imposed by DKIM.