Defending DKIM   IETF 65

Threats and Strategies

Douglas Otis
Doug_Otis@trendmicro.com

Trust Still at Risk with Base DKIM

- Resource Intensive Assessments!
- Not all Users are Secure and Trustworthy!
- Message Replay Abuse!
- Denial of Service Attack!
- Weak Visible Recognition of Email-Address!
Ascribing Bad Signers

• Limited to Message Content
  – Malware
  – Misleading Links
  – Misleading Information
  – Invalid Encompassed Header Fields
• Evaluation is Resource Intensive
• Undesired Messages Ignored
Reducing Resource Expenditures

- Use of Sub-Domains Adds Confusion
- Any Message Source Might Impact Trust
- Key Group Tags Can:
  - Indicate Unvetted Sources
  - Reduce Evaluation Costs
  - Retain Signing Domain Trust
  - Condition Message Level Precautions
Safe Recipient Assurances

• Message Annotation Can Overcome:
  – RFC 2047, 3490-3492 Unicode Repertoires
  – Unverified Display-Names
  – Confusing DNS Hierarchy
  – Visually Similar Characters or Ideograms
  – Non-Allied Email-Addresses
  – Lack of Email-Policy
• Annotation May Note Allied Email-Addresses
The Battle of the Zombies

- Zombies are a Primary Delivery Vehicle
- Rate Restrictions Countered with Replay
- Key Revocation is Not Practical
- Opaque-ID Convention for Reporting
- Self Opaque-ID Block-Listing for Scaling
**DKIM Denial Of Service Attack**

- EHLO Verification for Immediate Acceptance
- Signer Association with EHLO via PTR

\[
\text{_oa._smtp.<domain> PTR isp.net.}\*
\]

\[
\text{_dkim._smtp.<domain> PTR isp.net. ads.com.}\*
\]

\[
\text{_dkim._smtp.<domain> PTR .}\*
\]

"*." Open-ended, "." Empty & Closed-ended
Not describing the EHLO path has less value but...

Does email-address domain permit Third-Party Signers? (Rather than SSP yes/no assertion.)

_tps._smtp.<email-domain>. PTR <dkim-domain>.
<dkim-domain>. "*"
Limited Signature Roles Limit DoS Attack

Signature field \( w = b:(\text{Role} + \text{Binding}) \)
Key field \( w = <\text{group}> \)

Cached binding checked before conflict rejection:
\(<\text{group}>._\text{dkim-group}.<\text{domain}> \ A 127.0.0.2 \ (\text{binding})✓\)

Group name conventions:
- admin: (restricted access)
- user: (general access)
- guest: (unrestricted access)
- list: (list)
- auto: (auto-response)
- info: (promotional or general status information)
- test: (for test only)
- void: (no longer a valid group)
Signing Roles & Exclusivity Assertions
Signature Parameter 'w='

- Source of Signatures using two characters <source><exclusivity>
  For example, Sig Header: w=Sb
- SsMmDd/bn
  - (S) MSA Primary (Default)
  - (s) MSA Secondary
  - (M) Mediator Primary
  - (m) Mediator Secondary
  - (D) MDA Primary
  - (d) MDA Secondary
- Exclusivity Assertions (binding):
  - (b) Domain Always Signed (broad)
  - (n) Email-Address Always Signed (narrow)
Opaque-ID

Opaque-Identifier (persistent/sequential)
Signature field u=<p/s>-<redemption>-<uid>

<u>._dkim-revoke.<domain> A 127.0.0.2
Checks to Avoid DoS Attack

- If EHLO does not verify → Delay Acceptance (wl)
- If EHLO != DKIM-Domain → Check EHLO Association 
  _dkim._smtp.<dkim-domain> PTR for EHLO parent
- If No EHLO Association → Delay Acceptance (wl)
- If Delayed Acceptance Check for OID Revocation 
  <u>._dkim-revoke.<dkim-domain> for record
- If OID Revocation Record →Reject Message