DNS-based email security

Ralph Dolmans
Benno Overeinder
{ralph, benno}@nlnetlabs.nl
Industry partners

Fraunhofer IAO

Microsoft

Internet Systems Consortium

NLnet Labs

SECURE 64
Email exchange integrity is at risk

- Disclosure or modification of message.
  - STARTTLS (MTA-MTA)
  - StripTLS
- No source authentication.
  - S/MIME signing (MUA-MUA)
  - Have to trust all Certificate Authorities
  - Difficult to find certificates
Solution: Use DNS to bind keys to names

• TLS keys (TLSA)
• S/MIME (SMIMEA)

• Must validate using DNSSEC!
Solutions exist, but adoption is limited

• Guidance and recommendations needed

• NIST/NCCoE project:
  – Demonstrate using available standards-based software
Approach

• Map security characteristics to NIST best practices
  – NIST Special Publication 800-177 (SP800-177), Trustworthy Email

• Describe example solution, with instructions from implementers

• Evaluate example solution
Building blocks

• MUA
  - Microsoft Office, Thunderbird
• MTA
  - Postfix, Exchange
• DNS
  - NSD, Unbound, OpenDNSSEC
  - BIND, Secure64
Test environment

DNS-Based Email Security Test Set-up
## Test scenarios

<table>
<thead>
<tr>
<th>Sequence</th>
<th>NCCoE Lab</th>
<th>Legitimate Remote Site</th>
<th>Certificate on Receiver Side</th>
<th>Legitimate Remote Site</th>
<th>Certificate on Receiver Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>MUA</td>
<td>MTA</td>
<td>DNS Service</td>
<td>Secure 64</td>
<td></td>
</tr>
<tr>
<td>Event</td>
<td>Outlook</td>
<td>Exchange</td>
<td>Active Directory</td>
<td>Thunderbird on MacBook, Postfix/Dovecot, DNS Authority/Cache/Signer</td>
<td>Local CA (CU=1)</td>
</tr>
<tr>
<td>Event</td>
<td>Thunderbird</td>
<td>Postfix/ Dovecot</td>
<td>NSD4/ Unbound/ OpenDNSSEC</td>
<td>Same as 13</td>
<td>Local CA issued (CU=1)</td>
</tr>
<tr>
<td>Event</td>
<td>Thunderbird on MacBook</td>
<td>Postfix/ Dovecot</td>
<td>DNS Authority/Cache/Signer</td>
<td>Same as 13</td>
<td>Local CA issued (CU=1)</td>
</tr>
<tr>
<td>Event</td>
<td>Outlook</td>
<td>Exchange</td>
<td>Active Directory</td>
<td>Same as 13</td>
<td>Self-Signed Cert (CU=3)</td>
</tr>
<tr>
<td>Event</td>
<td>Thunderbird</td>
<td>Postfix/ Dovecot</td>
<td>NSD4/Unbound/ Open DNSSEC</td>
<td>Same as 13</td>
<td>Self-Signed Cert (CU=3)</td>
</tr>
<tr>
<td>Event</td>
<td>Thunderbird</td>
<td>Postfix/ Dovecot</td>
<td>BIND</td>
<td>Same as 13</td>
<td>Self-Signed Cert (CU=3)</td>
</tr>
</tbody>
</table>

[https://www.nlnetlabs.nl/](https://www.nlnetlabs.nl/)
DNSSEC enables verification of trust

• Test scenarios successfully executed!
• See: NIST Cybersecurity Practice Guide (1800-6)