Accessing Email services over TLS

Alexey Melnikov
<alexey.melnikov@isode.com>

IETF 88

Vancouver, BC

Table of Content

- Existing recommendations
- Real World
- What needs to be done in IETF

Current state of affairs – cipher suites

- RFC 2595: **TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA** is MUST implement for IMAP and **POP3**
- RFC 3501 (updated IMAP requirements): MUST implement **TLS_RSA_WITH_RC4_128_MD5** and SHOULD implement **TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA**
- RFC 3207: no cipher suite recommendation for **SMTP**
- RFC 5804: no cipher suite recommendation for **ManageSieve**

Current state of affairs – TLS server identity verification

- RFC 2595 (POP): Use dNSName subjectAltName in server certificate, wildcards are allowed in dNSName.
- RFC 3501 (IMAP): Same as in RFC 2595
- RFC 3207 (SMTP): “server certificate has a domain name that is the domain name that the client thought it was connecting to”
- RFC 5804 (ManageSieve): Use of SRVName and dNSName subjectAltName is recommended. CN in subject names is also supported. iPAddress subjectAltName is also supported.
- **Need to update these to use RFC 6125 profile(s)**

Real World

- <Extract info from Ned's email to perpass about what cipher suites are currently supported by ISPs>

Things to do (even without DANE)
1 of 2

- Update cipher suite recommendations. Recommend perfect forward secrecy cipher suites.
- Deprecate use of old SSL version (SSL2, SSL3?). Recommend TLS 1.2 [draft-moore-email-tls, Chris Newman's draft]
- Specify TLS server identity checks based on RFC 6125 profile [draft-melnikov-email-tls-certs]
- Properly document use of POPS and IMAPS ports [draft-melnikov-pop3-over-tls] ?
- A minor issue with port 465 (Submission over TLS) IANA registration
- Revise recommendations on use of TLS ports versa STARTTLS command? [draft-moore-email-tls]
- Recommend use of opportunistic encryption and describe how to implement it in clients [draft-moore-email-tls, Chris Newman's draft]

Things to do (even without DANE) 2 of 2

- Need to be able to record TLS cipher in the Received header field [Chris Newman's draft]

TLS server identity verification based on RFC 6125

- draft-melnikov-email-tls-certs-01, based on RFC 6125:
- Support dNSName subjectAltName (DNS-ID)
  - Use both for right hand side of email addresses and for the server hostname. This copes with different types of client configuration.
- Support SRVName subjectAltName (SRV-ID) in order to support RFC 6186 (Use of SRV Records for Locating Email Submission/Access Services)
- CN=<server-hostname> in subject name (CN-ID) is supported for backward compatibility
- Wildcards are allowed in the leftmost component of DNS-ID and CN-ID