Extensions to ACME for email (TLS, S/MIME)

draft-ietf-acme-email-tls-05
draft-ietf-acme-email-smime-04

Alexey Melnikov, Isode Ltd

Changes in draft-ietf-acme-email-tls-05 since London

- Moved “service” and “port” from “protected” to “payload”. Both are protected by the signature, but the latter contains other challenge related data.
- Added SMTP extension registration (required by the base SMTP spec)
- Corrected some typos

Open issues in draft-ietf-acme-email-tls-05

- Should the same ACME certificate be allowed to cover both TLS and non TLS ports? Multiple related services?
  - Change “service” and “port” to be arrays of values

Next step

- Anybody interested in implementing?
- Ask for feedback on SMTP and IMAP related mailing lists.
- Nearly ready for WGLC
  - After changing “service” & “port” to be arrays

Changes in draft-ietf-acme-email-smime-04 since London

- Spelled out how challenge and response email messages are generated in more details.
- Added some example messages.

Open issues in draft-ietf-acme-email-smime-04

- No fancy text/html or multipart/alternative for challenge and response messages?
  - Probably not text/html. Multipart/alternative is more reasonable (clients can display nice HTML if capable), but adds implementation complexity. Multipart/mixed can include a special media type attachment that can be used to invoke and external program on some platforms.
- How to validate email challenges sent by CA?
  - S/MIME signed? DKIM signed with valid SPF & DMARC?
- Similarly: how to very email responses? DKIM/SPF/DMARC?

Background slides

Email services running over TLS

- Goal: being able to get a certificate for SMTP submission, IMAP, etc servers
- According to **RFC 7817,** such certificates either contain **dNSName** or **srvName** in certificate's subjectAltName
  - srvName is nice, because it can limit protocols a certificate can apply to.
- Requirement: avoid the need to run an HTTP server on the same hostname in order to get an ACME certificate
  - One can just use base ACME protocol to get a certificate with dnsName and reuse it for email. ***But key usage in the certificate can be wrong.***

Email services running over TLS - proposals

- Options 1:
  - Extend DNS verifier to specify protocol and possibly port number
    - E.g. _993._imaps._acme-challenge.example.com
    - Pros: sysadmins running email services usually have DNS control over the corresponding domain (e.g. to set MX, SRV, DKIM and DMARC TXT records)
    - Cons: in some domains people controlling DNS and people controlling email services are different groups of people

Email services running over TLS - proposals

- Option 2:
  - Define extensions to SMTP/IMAP/POP3 to advertise proof of control over the corresponding SMTP/IMAP/POP3 service
    - Pros: no need to change/add DNS records
    - Cons: either need to restart SMTP/IMAP/POP3 service to publish “proof of control over domain” or might need to redesign the server to be able to publish such proof without restarting

S/MIME

- Goal: be able to get a certificate associated with an email address, which is suitable for S/MIME signing and/or encrypting
- Need a new Identifier Type (email address) and email specific challenge type
- Need some kind of proof of control over the email address: so some kind of challenge (email message sent to the email address) and response (reply email using a more or less standard email client), similar to what happens when subscribing to a mailing list?
  - If an attacker can control DNS, it can reroute email. Assuming that an email owner doesn't control DNS seem to be acceptable risk.

Thank You

- Comments? Questions? Offers to help out with this work? Hackathon?
- Talk to me offline or email me at alexey.melnikov@isode.com