HTTP SCRAM

draft-ietf-httpauth-scram-auth-00.txt

IETF 87, Berlin

Open Issues

- Does the "realm" attribute need to be repeated beyond the first response from the server/request to the server?
- Add "domain" attribute like HTTP Digest and other proposals?
- Should authentication exchange protect HTTP Method, Request URI and (optionally) message body (like HTTP Digest)?

Open Issues

- Should HTTP Digest's Authentication-Info Header Field be reused for the last leg of the auth exchange?
  - This might be a question for HTTPBis

Open Issues

- Send each request/response as a single HTTP attribute (as a quoted string) or send each SCRAM attribute as HTTP attribute?
  - E.g. Authorization: SCRAM-SHA-1 realm="testrealm@host.com", g=n,n=user,r=fyko +d2lbbFgONRv9qkxdawL
  - Or SCRAM-SHA-1 realm="testrealm@host.com", g=n, n="user", r="fyko+d2lbbFgONRv9qkxdawL"

To Do

- Quick reauthentication sequence needs to be specified (also an open issue)
- Need to specify normalization for usernames and password (most likely outcome of Precis WG)
- Cleanup some text which came originally from SASL SCRAM (channel bindings, comparison with other SASL mechanisms)