HTTP SCRAM

draft-ietf-httpath-scram-auth-03.txt

Changes since -01

- Outline of the 1-roundtrip reauthentication
- Fix examples (where sid and where realm directives are to be used) -- as per Tony Hansen comment
- Added proper hash function agility in ABNF (as per Tony Hansen)

Full authentication

- S: HTTP/1.1 401 Unauthorized
- S: WWW-Authenticate: Digest realm="realm1@host.com",
- SCRAM-SHA-1 realm="testrealm@host.com"
- S: [...]
- C: GET /resource HTTP/1.1
- C: Authorization: SCRAM-SHA-1 realm="testrealm@host.com", g=n,n=user,r=fyko+d2lbbFgONRv9qkxdawL
- C: [...]
- S: HTTP/1.1 401 Unauthorized
- S: WWW-Authenticate: SCRAM-SHA-1 sid=AAAABBBBCCCCDDDD,r=fyko+d2lbbFgONRv9qkxdawL3rfcNHYJY1ZVvWVs7j, s=QSXCR+Q6sek8bf92,i=4096
- S: [...]
- C: GET /resource HTTP/1.1
- C: Authorization: SCRAM-SHA-1 sid=AAAABBBBCCCCDDDD, c=biws,r=fyko+d2lbbFgONRv9qkxdawL3rfcNHYJY1ZVvWVs7j,p=v0X8v3Bz2T0CJGbJQyF0X+HI4Ts=
- C: [...]
- S: HTTP/1.1 200 Ok
- S: Authentication-Info: SCRAM-SHA-1 sid=AAAABBBBCCCCDDDD,v=rmF9pqV8S7suAoZWja4dJRkFsKQ=
- S: [...Other header fields and resource body...]

Reauthentication

- On initial authentication:

- C: GET /resource HTTP/1.1
- C: Host: server.example.com
- C: [...]
- S: HTTP/1.1 401 Unauthorized
- S: WWW-Authenticate: Digest realm="realm1@host.com",
-         SCRAM-SHA-1 realm="testrealm@host.com", **sr=3rfcNHYJY1ZVvWVs7j**
- S: [...]

Reauthentication

- Quick reauthentication (iteration counter and per user salt are cached from an earlier authentication exchange, "sr" becomes part of "r") - identical to the second leg of the full exchange.

- C: GET /resource HTTP/1.1
- C: Host: server.example.com
- C: Authorization: SCRAM-SHA-1 realm="testrealm@host.com",
- c=biws,r=fyko+d2lbbFgONRv9qkxdawL3rfcNHYJY1ZVvWVs7j,
- p=v0X8v3Bz2T0CJGbJQyF0X+HI4Ts=
- C: [...]

- S: HTTP/1.1 200 Ok
- S: Authentication-Info: SCRAM-SHA-1
- sid=AAAABBBBCCCCDDDD,
- v=rmF9pqV8S7suAoZWja4dJRkFsKQ=
- S: [...Other header fields and resource body...]

Open Issues

- Encode each request/response as base64 (easy compatibility with SASL SCRAM)

- Mandatory to implement hash function?

- Username/password canonicalization before hashing

    - Use StringPrepBis (Precis WG)?

        - http://tools.ietf.org/html/draft-ietf-precis-saslprepbis-06

Open Issues

- Maintaining session state (as SCRAM requires 2 round trips)
  - Use "sid" directive?
  - Use a separate header field (e.g. Microsoft's proposal: draft-montenegro-httpbis-multilegged-auth-01)?