HTTP SCRAM

draft-ietf-httpath-scram-auth-04.txt

Changes since -03

- Clarified how 1-roundtrip reauthentication works
- Added "ttl" attribute that signals how long the server nonce ("sr") is valid for

Full authentication (1 of 5)

Server advertises support for SCRAM

- S: HTTP/1.1 401 Unauthorized

- S: WWW-Authenticate: Digest realm="realm1@host.com", SCRAM-SHA-1 realm="testrealm@host.com"

Full authentication (2 of 5)

Server advertises support for SCRAM

- C: GET /resource HTTP/1.1

- C: Authorization: SCRAM-SHA-1 realm="testrealm@host.com", g=n,**n=user,r=fyko+d2lbbFgONRv9qkxdawL**

- Or

- C: Authorization: SCRAM-SHA-1 realm="testrealm@host.com", data=base64(n,,**n=user,r=fyko+d2lbbFgONRv9qkxdawL**)

- The latter is base64 of the first client message from the SCRAM RFC, the former is a modified version that fits HTTP syntax.

Full authentication (3 of 5)

Server returns user specific parameters

- S: HTTP/1.1 401 Unauthorized

- S: WWW-Authenticate: SCRAM-SHA-1 sid=AAAABBBBCCCCDDDD,**r=fyko +d2lbbFgONRv9qkxdawL3rfcNHYJY1ZVvWVs7j, s=QSXCR +Q6sek8bf92,i=4096**

- Or

- S: WWW-Authenticate: SCRAM-SHA-1 sid=AAAABBBBCCCCDDDD,data=base64(**r=fyko +d2lbbFgONRv9qkxdawL3rfcNHYJY1ZVvWVs7j, s=QSXCR +Q6sek8bf92,i=4096**)

Full authentication (4 of 5)

Client sends password verifier

- C: GET /resource HTTP/1.1

- C: Authorization: SCRAM-SHA-1 sid=AAAABBBBCCCCDDDD, **c=biws,r=fyko +d2lbbFgONRv9qkxdawL3rfcNHYJY1ZVvWVs7j,p=v0X8v3 Bz2T0CJGbJQyF0X+HI4Ts=**

- Or

- C: Authorization: SCRAM-SHA-1 sid=AAAABBBBCCCCDDDD, data=base64(**c=biws,r=fyko +d2lbbFgONRv9qkxdawL3rfcNHYJY1ZVvWVs7j,p=v0X8v3 Bz2T0CJGbJQyF0X+HI4Ts=**)

Full authentication (5 of 5)

Server sends its mutual authentication proof

- S: HTTP/1.1 200 Ok
- S: Authentication-Info: SCRAM-SHA-1 sid=AAAABBBBCCCCDDDD,**v=rmF9pqV8S7suAoZWja4dJRkFsKQ=**
- Or
- S: Authentication-Info: SCRAM-SHA-1 sid=AAAABBBBCCCCDDDD,data=base64(**v=rmF9pqV8S7suAoZWja4dJRkFsKQ=**)

1 round trip Reauthentication (1 of 3)

Server advertises support for SCRAM

- S: HTTP/1.1 401 Unauthorized

- S: WWW-Authenticate: Digest realm="realm1@host.com",

- SCRAM-SHA-1 realm="testrealm@host.com", **sr=3rfcNHYJY1ZVvWVs7j, ttl=360**

1 round trip Reauthentication (2 of 3)

Client sends password verifier

- 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, but includes "realm" instead of "sid"

- C: GET /resource HTTP/1.1

- C: Authorization: SCRAM-SHA-1 realm="testrealm@host.com", **c=biws,r=fyko +d2lbbFgONRv9qkxdawL3rfcNHYJY1ZVvWVs7j,p=v0X8v3Bz2T0CJGbJQyF0X+HI4Ts=**

- Or

- C: Authorization: SCRAM-SHA-1 realm="testrealm@host.com", data=base64(**c=biws,r=fyko +d2lbbFgONRv9qkxdawL3rfcNHYJY1ZVvWVs7j,p=v0X8v3Bz2T0CJGbJQyF0X +HI4Ts=**)

1 round trip Reauthentication (3 of 3)

Server sends its mutual authentication proof

- S: HTTP/1.1 200 Ok

- S: Authentication-Info: SCRAM-SHA-1 sid=AAAABBBBCCCCDDDD,**v=rmF9pqV8S7suAoZWja4dJRkFsKQ=**

- Or

- S: Authentication-Info: SCRAM-SHA-1 sid=AAAABBBBCCCCDDDD,data=base64(**v=rmF9pqV8S7suAoZWja4dJRkFsKQ=**)

Open Issues

- Encode each request/response as base64 (easy compatibility with SASL SCRAM)?
- Need to clarify some details in reauthentication exchange
- Mandatory to implement hash function?
  - Suggested resolution: SHA-256
- 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)?