Salted Challenge Response Authentication Mechanism (SCRAM)

draft-newman-auth-scram-06.txt

Abhijit Menon-Sen <ams@oryx.com>
Chris Newman <chris.newman@sun.com>
Alexey Melnikov <alexey.melnikov@isode.com>

IETF 73, Minneapolis
Resolved Issues (1 of 5)

• Text about channel binding handling is incomplete (missing references) and might be wrong. Should the channel binding data be sent by the client, by the server, or both?
  – Nico said the current text is Ok and we trust him :-)
Resolved Issues (2 of 5)

• Hashed algorithm negotiation removed, so the draft now defines a family of SCRAM-HMAC mechanisms, e.g. SCRAM-HMAC-SHA-1
  – The document uses the IANA registry created by RFC 4572 (<http://www.iana.org/assignments/hash-function-text-names/hash-function-text-names.xhtml>)
  • All registered hashes are in lowercase (e.g. “sha-1”), but SASL mechanism names only allow for upper case letter
  • The registry doesn't seem to define ABNF for allowed hash names
Resolved Issues (3 of 5)

• Clarified extensibility
  – Unrecognized attributes are ignored
  – Except for the “m” attribute which defines mandatory extensions that must be understood by the other end
• Syntax is unspecified
Resolved Issues (4 of 5)

- Hi(str, salt):
  - $U_0 := \text{HMAC} (\text{str}, \text{salt})$
  - $U_1 := \text{HMAC} (\text{str}, U_0)$
  - ...
  - $U_{i-1} := \text{HMAC} (\text{str}, U_{i-2})$
  - $U_i := \text{HMAC} (\text{str}, U_{i-1})$

- Hi := $U_0 \text{ XOR } U_1 \text{ XOR } U_2 \text{ XOR } ... \text{ XOR } U_i$

- where "i" is the iteration counter.

- PBKDF2 (P, S, c, dkLen)
  - Options: PRF - underlying pseudorandom function (hLen) denotes the length in octets of the pseudorandom function output

- Input: P - password, an octet string
  - S - salt, an octet string
  - c - iteration count, a positive integer
  - dkLen - intended length in octets of the derived key, a positive integer, at most $(2^{32} - 1) \times \text{hLen}$

- Output: DK derived key, a dkLen-octet string

- Hi(str, salt) = $T_1 = F (\text{str}, \text{salt}, c, 1)$
  - $U_1 = \text{PRF} (\text{str}, \text{salt} \| \text{INT} (1))$
  - $U_2 = \text{PRF} (\text{str}, U_1)$,
Resolved Issues (5 of 5)

• Standardize LDAP attribute for storing SCRAM authentication information
  – draft-melnikov-sasl-scram-ldap-00.txt defines `saslSecretScram` multivalue attribute
    
    ```
    scram-secret = hash-mech "$"
    iter-count "$" salt "$" stored-key "$" server-key
    
    hash-mech = "hmac-sha-1"
    iter-count = %x30-39 *DIGIT
    salt value
    stored-key value
    server-key value
    ```
Examples need to be written.
Open Issues

• GS2 framing?