Salted Challenge Response Authentication Mechanism (SCRAM)

draft-newman-auth-scram-10.txt

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

IETF 74, San Francisco

Status

- Nearly ready for WGLC, but need to choose between purt-SCRAM and SCRAM-as-GS2 variants
- A couple of implementations of SCRAM exist (Dave Cridland, Alexey)

Major Changes since -07

- ***Moved authorization identity to the second message from the client***
- ***Clarified the meaning of the "m" option (mandatory future extensions)***
- ***Clarified handling of the "c" (channel binding data) option***
  - ***Unrecognized channel bindings are ignored by the server***
- ***Allow CTL, but disallow NUL in authentication and authorization identities***
- ***Added some text on comparison with CRAM-MD5***
- ***Added description of design goals***

Open Issues (1 of 4)

- Min/Recommended iteration counter value
  - Simon has recommended to use 4096
  - Dave Cridland has suggested that clients can cache SaltedPassword after the first authentication to a server
    - Some text on this needs to be added to the document
- Key derivation
  - Currently:
    - ClientKey = H(SaltedPassword)
    - ServerKey = HMAC(SaltedPassword, salt)
  - Should this be something like:
    - ClientKey = HMAC(SaltedPassword, "Client Key")
    - ServerKey = HMAC(SaltedPassword, "Server Key")

Open Issues (2 of 4)

- Use of service name/URI in SCRAM
  - Can prevent an attack when user credentials are used by a bad server to connect to another server using the same password/salt
  - This is a weaker protection compared to channel bindings
  - A similar construct caused problems in DIGEST-MD5 implementations

Open Issues (3 of 4)

- ***GS2 framing ?***
  - ***Jeff and Nico have a new design with just one all text header to client's first authentication message and to the channel binding (CB) data.***
  - ***See slides from Nico***

Open Issues (4 of 4)

- ***Issues related to GS2 variant:***
  - ***One or two SASL mechanism names (+ a bit saying which ones were advertised)***
    - ***One mechanism name indicates that server can do channel bindings (CB), one indicates it can't***
    - ***The GS2 1st client message/CB data header includes a flag indicating whether the client couldn't, could have, or did do CB***