IETF 61

draft-sterman-aaa-sip-04

Wolfgang Beck
Deutsche Telekom AG

Response-auth

- new attribute Digest-HA1
- only allowed if
  - it was calculated using random components: MD5-sess, AKA-MD5-sess
  - or there is a secure connection between RADIUS client and RADIUS server
- no objections so far

Digest-HA1

- MD5:
  H(username “:” realm “:” password)
  - no random components, replay attacks possible
- MD5-sess:
  H(H(username) “:” realm “:” passwd)
  “:” nonce “:” cnonce)
  - better

Message-Authenticator

- RfC 3579 is nice, but Informational
- added to -04 as a 'MAY'

What is a 'secure connection'?

- added some clarifications
- RADIUS clients/servers can't decide how secure their connection is
- operator must make sure that RADIUS traffic can't be tapped or modified
- IPSEC is one way to secure connections

sips/https and RADIUS

- sips and https user expect that hops don't send message (or parts) in the clear
- clear text RADIUS would reveal URIs and methods

Access-Challenge

- in -03, the RADIUS server sent nonces in an Access-Accept
- Access-Challenge is more natural for this task

Diameter SIP application

- draft-sterman can't rely on encrypted connections, so some operation modes of diameter-sip-app would not be secure
- draft-sterman concentrates on authentication

Editorial

- some rearrangements in motivational and overview sections
- fixed and simplified examples
- added HTTP examples
- fixed typos, misleading references

IANA considerations

- a IANA request has been submitted long ago, but received no decision yet
- to make Diameter gateway implementation easy, attribute values should correspond between RADIUS and Diameter
- Authors will meet this week to align the work

Thanks to all reviewers!

Jari Arkko
Miguel Garcia
Avi Lior
Pete McCann