Support of fragmentation of RADIUS packets

draft-perez-radext-radius-fragmentation

IETF85 – RADEXT

Diego R. Lopez - Telefónica (diego@tid.es)

Status

- -05 submitted for WG adoption review
- Comments addressed in -06
  - Though not published yet
- Including
  - Comments to the fragmentation mechanism description
  - Clearer discussion on the addressed use cases and alternatives in the introduction
  - Satisfy ABFAB requirements on supporting chunked data transfer prior to the authentication flow

WG Adoption

- Comments on the problem statement and the rest of the text addressed in replies through the mailing list
  - And a solution acceptable to ABFAB discussed among authors
- -06 is updated according to this replies
- Shall we consider this is enough for rough consensus on WG adoption?

AuthN and AuthZ

- A RADIUS conversation is decomposed in three phases:
    1. RADIUS pre-authentication authorization (like a SAML request expressing a required LoA)
    2. RADIUS authentication (like standard RADIUS-EAP)
    3. RADIUS authorization (like a SAML response)
    - Phases are bound through *references* (e.g. State attribute).
    - Phase (1) finishes with a token which is used in the `Access-Request` for phase (2).
    - Phase (2) finishes with a token in the `Access-Accept`, which refers to phase (3).
- Fragmentation is supported in phases 1 and 3
    - Phase 2 is unaltered
- Fragmentation is based on `Access-Request/Access-Accept` rounds

Implementation Goals

- Implement draft-perez-radext-radius-fragmentation
  - Serve as a proof of feasibility
  - Provide on-the-wire feedback for the specification
- Proof of concept
  - Intended for validating the fragmentation mechanism
- Open source
  - Source code contributed to FreeRADIUS and available upon request

Implementation Details

- Based on FreeRadius 2.1.12
  - Client based on FreeRadius `radeapclient`
- Currently implements -04
  - Will be updated accordingly once consensus is reached
- Works through out-of-the-box FreeRadius proxies
  - No need of RADIUS fragmentation support on existing/deployed proxies