draft-perez-radext-radius-fragmentation

IETF 84 - Vancouver

Most Important Changes in -02

- **Overview section improved**
  - Now it indicates that this kind of fragmentation is most likely to occur due to an authorization exchange happening after authentication has been completed.
- **Description of the process**
  - Better organization of the subsections
  - ID field included in the examples, as it is used by the client to keep track of paired Request/Response packets
- **Added discussion about the chunk size**
  - Explains why chucks cannot have exactly 4096 bytes payload
    - RADIUS attributes have variable size.
    - Chunks require extra attributes for signaling
      - More-Data-Pending and State (**and User-Name!!**)
    - MTU
    - Proxy-State attributes
  - Includes the description of the mechanism for the client to discover the amount of included Proxy-State attributes along the path to the server

Most Important Changes in -02

- **State attribute**
  - New section added describing how to deal with State attribute already present into the original packet
- **Proxies**
  - New section discussing implications when leading with proxies (this was in the presentation I made in Paris, but not in the previous draft)
- **Security considerations**
  - Added a paragraph indicating that it is assumed that proxies are considered trusted entities (they can make fragmentation fail if they want)

And More To Come: User-Name

- We have found we need to add User-Name to any Access-Request message
  - Let Proxies to be able to forward the chunks to their proper destination.
  - Stated in RADIUS EAP, where User-Name MUST be included in every Access-Request packet
- Update fragmentation procedures to include
  - Access-Request

```
If the original Access-Request packet contains a User-Name attribute, it MUST
be included on every CHUNK sent to the server. This is required so Proxies
may need this value to forward the CHUNK to the proper server.
```

  - Access-Challenge

```
If the original Access-Request that motivated the generation of the
fragmented Access-Challenge contained a User-Name attribute, the RADIUS
client MUST include this value on every "CHUNK request" message it sends.
That is, every "chunk request" message would contain the received State
attribute and the User-Name.
```