networkRADIUS

ALPN for RADIUS

MD5 IS DEAD

ALAN DEKOK IETF 116

USE APPLICATION-LAYER PROTOCOL NEGOTIATION

- Start with (D)TLS
- Port 2083
- Add ALPN negotiation
- Can do different application-layer protocols

GOAL: remove dependency on MD5

PROFILE: RADIUS/V1.1

- User-Password etc. are encoded as “text”, protected by TLS.
  - Message-Authenticator is ignored
  - CHAP, MS-CHAP, etc. can still be transported
- No changes to other attribute encoding

TRANSPORT != AUTHENTICATION METHODS

- Proxies do not decode or interpret CHAP, etc.
- Home servers control which authentication methods they support
- Changing the transport method does not change the data being transported
- Avoiding MD5 for client -> server TLS connections means:
  - that session can still transport MD5-related data
  - The home server can still do MD5 hashes on CHAP, etc.

REPURPOSE THE AUTHENTICATOR FIELD

- 16-octet unused field in the packet header
- Add 32-bit request / reply token (extended ID)
- Add flags:
  - Client Security - this packet used secure transport
  - Server Security: Require secure transport for replies
- Implemented in GitHub branch. ~2K diff

CHANGES FROM SRADIUS

- SRADIUS bad, ALPN good!
- Many more cleanups and checks around corner cases
- Many more explanations of corner cases and guidance to implementors
- The document is pretty close to being done