RADIUS over TLS
Status of draft

- WGLC completed; in PROTO writeup
- Some unresolved comments
  - Client Identity
  - Packet flow Client -> Server and vice versa
  - Connection backoff
- The end is nigh?
Client Identity

• We've been here before...

• Problem: there are many attributes in a X.509 certificate which can be used to classify connecting clients

  • Be open, by stating „it SHOULD be configurable which of those attributes a deployer considers for denoting a client's identity?"

  • Or: provide a „default“ identity scheme, like „the CN in combination with the issuing CA uniquely identifies a client“?

  • Or: make it someone else's problem: draft-saintandre-tls-server-id-check-08
Packet flow constraints

- **RADIUS/UDP**: sessions flow one way
  (Client sends Access-Request, Server replies with Access-Accept)

- **RADIUS/TLS**: transport creates bidirectional channel
  
- In combination with dynamic discovery, server might think it's a good idea to forward Access-Requests for certain realms to the Client
  
- That shouldn't be allowed to happen

- Text right now enumerates packet types which can flow in the respective directions

- There might be more elegant wording.
Example
RADIUS/TLS + dynamic discovery

WiFi AP

Server
realm=evil.com

User
...@edu.lu

Server
realm=edu.lu

User
...@evil.com

WiFi AP
Connection backoff

- What happens if a client attempts to connect to a server, but fails?
  - Retrying immediately could generate DoS
  - Backing off is required
  - Define and put into Security Considerations

- Will check text in Status-Server and use that or produce new text.