eduroam at the IETF

tnc32 Mobility Day | 09.06.2023

Jan-Frederik “Janfred” Rieckers

What happened

- radext WG was closed prior to IETF 113 (Vienna, March 2022)
- Recharter initiated by Alan DeKok and others
- BoF session at IETF 115 (London, November 2022)
- Charter approved just prior to IETF 116 (Yokohama, March 2023)

But why?

- RADIUS still uses MD5 for „Security“ (C’mon, it’s 2023. Really?)
  - Not really FIPS-compliant.
- RADIUS/UDP is used everywhere.
- RADIUS/(D)TLS is officially still an experimental standard
- RADIUS is missing „traceroute“ feature

Timeline

- Aug 2023 – RADIUS v1.1, *reverse CoA*
- Sep 2023 – TLS-PSK Best Practices for RADIUS/(D)TLS
- Jan 2024 – RADIUS/(D)TLS as Proposed standard, deprecate insecure RADIUS transports
- May 2024 – multihop status / traceroute, *extend 8-bit ID-Space*

RADIUS v1.1

- Get rid of MD5
  - RADIUS/(D)TLS mandatory, shared secrets are not needed any more
- Drop obfuscation of attributes (MSPPE-Keys, Passwords, …)
- Drop Auth mechanisms (Request Authenticator, Message Authenticator)
- Use Request/Response authenticator for ID
  - Extends current 8-bit ID space, now up to 2^32 packets in-flight possible
- Intended status: „Experimental“, FreeRADIUS Implementation available
- https://datatracker.ietf.org/doc/draft-ietf-radext-radiusv11/

TLS-PSK best practices

- Certificates are hard
- RADIUS/(D)TLS allows TLS-PSK, but does not say how
- RADIUS/(D)TLS with TLS-PSK should be easy if you already have a process for shared secrets
- Make things more secure! (It’s 2023, are we really still sending unencrypted personal information across the Internet? Outer Username, MAC-Address of Client+AP, …)
- https://datatracker.ietf.org/doc/draft-dekok-radext-tls-psk/

RADIUS/(D)TLS

- RFC6614 and RFC7360 are still Experimental
- Make TLSv1.2 MANDATORY, TLSv1.3 RECOMMENDED
- Add more text for TLS-PSK, add spec for raw public keys
- More explicit specification for certificate verification
- Merge RADIUS/DTLS, RADIUS/TLS and some of RADIUS/TCP
- https://datatracker.ietf.org/doc/draft-rieckers-radext-rfc6614bis/

Multihop / Traceroute Status

- RADIUS is Hop-by-Hop. How do you find out where the problem is?
  - My institution? My NRO? The other NRO? The home institution of the user? Someone else?
- Introduce new RADIUS messages for probing RADIUS Routing Path
  - Ping + Traceroute
  - What else do we need?
- https://datatracker.ietf.org/doc/draft-cullen-radextra-status-realm/

Discussion/Questions?

- Contact
  - Jan-Frederik Rieckers

Mail: rieckers@dfn.de
Phone: 0049 30 884299-339
Fax: 0049 30 884299-370

Address:
DFN-Verein, Geschäftsstelle
Alexanderplatz1
10178 Berlin