IETF update

tnc24 Mobility Day | 10.06.2024

Jan-Frederik “Janfred” Rieckers

What's happening

- New radext WG active since November 2022
  - Fix everything that is wrong with RADIUS (if possible)
- emu WG recharter
  - Recharter is currently in community review to incorporate some new work

radext Timeline

Moved to new milestone, some time in 2024. hopefully.

- ~~Aug 2023~~ Mar 2024 – RADIUS v1.1 (Submitted to IESG), ~~*reverse CoA*~~
- ~~Sep 2023~~ Feb 2024 – TLS-PSK Best Practices for RADIUS/(D)TLS (Submitted to IESG)
- ~~Jan 2024~~ End of 2024? – RADIUS/(D)TLS as Proposed standard (still in discussions), deprecate insecure RADIUS transports (still in discussions)

See Blast!RADIUS for this one

- ~~May 2024~~ ??? – multihop status / traceroute (still in discussions), ~~*extend 8-bit ID-Space*~~

Achieved with RADIUS v1.1, so probably we'll ignore this

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 built-in integrity protection mechanisms (Response Authenticator, Message Authenticator Attribute). That’s what we have TLS for.
- 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/
- Submitted to the IESG, AD review received yesterday. (need to update some text)

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
- TLS-PSK is implemented in FreeRADIUS (for a while now) and in radsecproxy (since version 1.11.0-rc1. Please test it!)
- Submitted to the IESG, need to change some text after AD review

RADIUS/(D)TLS and deprecating RADIUS/UDP

- 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
- TLS and DTLS is now mandatory for servers, clients can choose.
- Merge RADIUS/DTLS, RADIUS/TLS and some of RADIUS/TCP
- Use TLS best practices RFC for guidelines on using TLS
- https://datatracker.ietf.org/doc/draft-ietf-radext-radius-dtls-bis/
- „Deprecating insecure usages of RADIUS“ draft will be published arround the same time

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?
- Draft is somewhat quiet, needs some more input. If you have opinions: Please share them! (either directly on the mailing list or with me as proxy)
- https://datatracker.ietf.org/doc/draft-cullen-radextra-status-realm/

emu Recharter (still under comunity review)

- TEAP-bis is finally finished and now in IESG review.
  - (Do we care? Does anyone do TEAP?)
- EAP-EDHOC for usage in constrained environments
  - EDHOC => Ephemeral Diffie-Hellman Over COSE
- Bootstrapped EAP-TLS using TLS-POK (proof of knowledge)
  - similar to DPP (Device Provisioning Protocol)
- EAP-FIDO
  - Is listed in charter as work item/deliverable
  - Still waiting for liaison connection to FIDO alliance
  - See our talk on Wednesday

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