RADEXTRA BoF@ IETF 115

Nov 7th 2022 1300 UTC
Mezzanine 1-4 Room

Chair: Stephen Farrell

https://datatracker.ietf.org/group/radextra/about/
Mailing list: https://www.ietf.org/mailman/listinfo/radext
Meeting Materials: https://datatracker.ietf.org/meeting/115/session/radextra
Chat: https://zulip.ietf.org/#narrow/stream/radextra
Etherpad (notes): https://notes.ietf.org/notes-ietf-115-radextra

Note Well

A reminder of IETF policies.

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

By participating in the IETF, you agree to follow IETF processes and policies.

If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.

As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.

Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

BCP 9 (Internet Standards Process)

BCP 25 (Working Group processes)

BCP 25 (Anti-Harassment Procedures)

BCP 54 (Code of Conduct)

BCP 78 (Copyright)

BCP 79 (Patents, Participation)

https://www.ietf.org/privacy-policy/ (Privacy Policy)

Agenda

1. Intro (chair, 5 mins)

   (Note taker/mic-line/agenda-bash)

2. Things to do:

   2.1: Background and Things to do (Alan DeKok, 25 mins)

   2.2: RADIUS/TLS (RFC6614) update (Jan-Frederik Rieckers, 10 mins)

   2.3: RFC 6421: Roadmap to Securing RADIUS (Bernard Aboba, 15 mins)

3. Possible mode of operation for a WG (chair, 5 mins)

   (Describing how virtual interims work well nowadays)

4. Charter text discussion (all, 30 mins)

5. The usual BoF questions (chair, 10 mins)

6. AD summary (Paul Wouters, 5 mins)

WG forming

- The intent of the BoF proponents is that this be a "WG forming" BoF

- If all goes well (today) that'd mean subsequent charter text tweaking on the mailing list...
  - ...then handing things over to an AD who'll progress things from there

- If things don't go well today then people can always go to the bar and try again later:-)
  - Process minutae: you can't try the same thing loads of times

- What does "go well" mean? See "the usual questions" we'll get to later

Possible Modus Operandi

- Many working groups these days use virtual interim meetings to make progress between IETF meetings and so those who can't travel are less discommoded

- Many working groups these days use github repos, PRs and issue tracking as they progress drafts

- Both of those might help a lot for a group that previously suffered from sporadic input

Draft Charter (1)

The RADIUS Extensions Working Group will focus on extensions to the RADIUS protocol pending approval of the new work from the Area Director and clarify its usage and definition.

Furthermore, to ensure backward compatibility with existing RADIUS implementations, as well as compatibility between RADIUS and Diameter, the following restriction is imposed on extensions considered by the RADEXT WG:

- All documents produced must specify means of interoperation with legacy RADIUS and, if possible, be backward compatible with existing RADIUS RFCs, including RFCs 2865-2869, 3162, 3575, 3579, 3580, 4668-4673,4675, 5080, 5090, 5176, 6158, 6421, 6613, 6614, 6911, 6929, 7360, 7585, 8044, and 8669.
- Transport profiles should, if possible, be compatible with RFC 3539.

The WG will review its existing RFCs' document track categories and where necessary or useful change document tracks, with minor changes in the documents if needed. Any changes to document tracks require approval by the responsible Area Director.

Charter text is exactly what's at:
https://datatracker.ietf.org/doc/bofreq-dekok-bofreq-dekok-radius-extensions-and-security-00/

Draft Charter (2)

Work Items

The immediate goals of the RADEXT working group are to address the following issues:

- Deprecating UDP as a transport for RADIUS outside of secure networks. This work updates RFC 6421.

- Moving RFC 6613 (RADIUS/TCP), RFC 6614 (RADIUS/TLS), and RFC 7360 (RADIUS/DTLS) to Standards track. Mandate the use of TLS 1.3. Adding TLS Server Name Indication to TLS-based transports.

- Define best practices for RADIUS roaming, and roaming consoortiums using based on experience with RADIUS/TLS.

- extend the 8-bit RADIUS ID space to allow more than 256 "in flight" packets across one connection. No changes to packet format are permitted.

Draft Charter (3)

Work Items (cont'd)

- Allow for CoA / Disconnect packets to be sent in "reverse" down a RADIUS/TLS or RADIUS/DTLS connection. This functionality permits the forward and reverse path to be identical, and assists with transit of NATs.

- TBD - Add a 64-bit "date" type. The "date" type is a 32-bit unsigned value, so it has a Y2106 problem, not a Y2038 problem.

- Defining a secure variant of RADIUS which does not use deprecated cryptographic methods such as MD4 and MD5. This variant will be suitable for use in a FIPS compliant system. The transport will be required to be TLS or DTLS. The packet format is unchanged from RADIUS. However, the packets no longer need to be signed. The attribute format is unchanged from RADIUS. However, attributes such as User-Password no longer need to be obfuscated, and can be sent as-is. Attributes which require MD4 or MD5 are forbidden. In short, "RADIUS without MD4 or MD5".

The Usual Questions

- "Usual questions" is a bit wrong – haggling over the questions is almost mandatory, so now's the time for that:-)
- Planned questions are (or were:-):

1) Is the problem statement clear, well-scoped, solvable, and useful to solve?

2) Is the IETF the right place for such work?

3) Who is willing to review drafts?

4) Who is willing to edit drafts?

5) Should the IETF form a WG with this charter?

> Assume charter text changes for which we seemed to have rough consensus today get implemented correctly (that can be confirmed on-list)

Note: I'll probably switch screens/tools if editing questions, so the above might not be what ends up being asked – check the meeting minutes to see!

Finishing up for today...

- AD wrap up/comments/questions
- Thanks!