Open Issues

RADEXT - IETF 94

Alan DeKok <aland@freeradius.org>

Open Issues

- A few issues / errata have been filed
  - 4369 (rejected) text on RFC 2548 MS-CHAP-MPPE-Keys
  - 4488 (rejected) RFC 2866 Acct-Session-Id
  - 4485 (verified) RFC 2866 Acct-Status-Type

MS-CHAP-MPPE-Keys

- MS-CHAP-MPPE-Keys is obfuscated using the same method as User-Password
- There are **no** provisions for determining length of clear-text data
- For User-Password, it's the first non-zero octet?
- MS-CHAP-MPPE-Keys is binary so we can't use the same (unspecified) method…

MS-CHAP-MPPE-Keys

- We need to either:
- a) Update RFC 2865 to discuss how to calculate the length of User-Password
- b) update RFC 2548 to discuss how to calculate the length of MS-CHAP-Error-Keys

Acct-Session-ID

- RFC 2866 suggests a scheme for creating Acct-Session-Id.
  - Part of which is a simple incrementing ID
- In practice, implementations re-use IDs
  - A lot. All the time.
- This makes it difficult to track user sessions

Acct-Session-ID

- Why does it matter to have a non-unique ID?
- Maybe the NAS rebooted (and you lost that packet)
- If you have user@example.com and session ID "00000000", which session is it for?
  - Before or after the reboot?
- This is an artificial example… it gets worse with 10^7 users

A Proposal

- Suggest that Acct-Session-Id be globally and temporally unique
  - Just like Request Authenticator
- This will not change existing implementations
- But we hope new / updated implementations will work better
- The nice thing is that Acct-Session-Id is an opaque token and has no internal meaning

Discussion

- There was a fair amount of discussion around the errata
  - Pro: this change affects only the NAS, and makes life easier for servers
  - Con: the spec is fine.

Question:

- What do do next?
- Ignore it?
- Issue an updated RFC?
- Errata is arguably the wrong place to do this?

Acct-Status-Type

- Many vendors are using Acct-Status-Type = On/Off for **subsystem** reboot.
- At the minimum, this breaks the principle of least surprise.
  - The NAS rebooted? No, only part of it!
- Uh… how do you tell **what** rebooted?
  - No standard means any meaning is implementation defined

Acct-Status-Type

- Errata should probably say no more than "Don't Use On/Off for subsystem reboot"
- I filed a request for IANA allocation of Subsystem-On and Subsystem-Off
  - Which mean… something
  - But are at least better than re-defining an existing value for Acct-Status-Type
- Designated expert is… who?

Conclusions

- RADIUS (still) isn't perfect
- Push from implementors / administrators to fix problems
  - Vendors often just use what seems to work, even if it's arguably wrong, or violates the spec
- Will likely not get a lot of feedback from vendors about what they want

Conclusions (2)

- Will need feedback from IEEE
- Due to updates for content of accounting messages
  - RFC 3580 makes recommendations, which need updating

Discussion?