RADEXT Meeting
IETF 85
Atlanta, USA

Tuesday 6 Nov 2012
Meeting started 3:22PM and adjourned 4:40PM

Chairs:

Jouni Korhonen <jouni.nospam@gmail.com>
Mauricio Sanchez <mauricio.sanchez@hp.com>

Agenda:

RADEXT WG IETF 85; 90 min

- 3:20 – 3:40 PM, Preliminaries (20 minutes)
  - Note Well, Note Takers, Jabber scribe
  - Agenda bash
- Document Status
- WG draft discussion (15 minutes)
  - 3:40 – 3:55PM RADIUS Attributes for IEEE 802 Networks, Bernard Aboba (15 minutes) http://tools.ietf.org/id/draft-aboba-radext-wlan
- Individual draft discussion (45 minutes)
  - 3:55 – 4:10PM Capability Negotiation in RADIUS, Alan DeKok (15 minutes) http://tools.ietf.org/html/draft-halwasia-radext-capability-negotiation-00
  - 4:10 – 4:25PM RADIUS accounting via IPFIX, Alan DeKok (15 minutes) http://tools.ietf.org/html/draft-dekok-radius-ipfix-00
  - 4:25 – 4:40PM Support of fragmentation of RADIUS packets, Diego Lopez (15 minutes) http://tools.ietf.org/html/draft-perez-radext-radius-fragmentation
- Wrap-up (10 minutes)
  - 4:40 - 4:50 PM Next Steps: WG Chairs & ADs

Minutes: Dorothy Stanley (Aruba Networks)

1. Chair reviewed agenda: no changes

2. Chair reviewed milestones; we are delinquent on charter dates. Proposing updated dates.
   a. Steve Hanna – correction – Typo on date for DTLS draft date is in 2013
   b. Alan – question on experimental status for RADIUS over DTLS.
   c. Joe S: Agree it should be experimental. What is issue with crypto-agility?
   d. Bernard – Distinguish DTLS from RADIUS packet. Upgrade path for legacy to DTLS, going forward.
   e. Alan – It is in the current draft.
   f. Chair: Propose that RADIUS extensions for traffic statistics be left for the future. Close in on the existing milestones ASAP, and work items that are close.
   g. Chair – Summary of RADEXT draft status; plan to go to WGLC as soon as possible on RADIUS over DTLS and NAI-based peer discovery drafts. Finish off current charter, and then recharter, - a lot of work going on in new items that are not in current charter – goal is to re-charter.
   h. Agree, believe combining drafts logical next step.

3. RADIUS Attributes for IEEE 802 Networks, Bernard Aboba presentation
    a. Summary of changes since -02. Includes resolution to issue 1-0, changes to section 2.14.
        i. Resolution to Issue 109
        ii. Changes in Section 2.14 (WLAN-Reason-Code)
        iii. Inclusion in Access-Reject or Disconnect-Request
        iv. Mapping of WLAN-Reason-Code to Acct-Termination-Cause for use in Accounting-Requests
    b. Is there any analog to this in 802.1X-2012?
    c. Don't think so. There is the network announcement piece. Premature to assign.
    d. New issue 130 – review on behalf of IEEE 802.11 by Dan Harkins.
        i. Review on behalf of IEEE 802.11 by Dan Harkins:
        ii. "I question the validity of using ciphersuite information and RF band to decide whether to accept/deny an authentication. If the AP is beaconing out support for a cipher that is not acceptable for RADIUS authentication by any user then it indicates a configuration error on the AP. Why on earth would one prohibit a user from a certain band that the AP is operating in? I think there should be some text around the utility of these attrs.
        iii. If you're gonna limit/prohibit people to/from "TV white space" then what channels in that space? Again, why?
        iv. The security considerations are pretty weak. Which of these new attributes need channel binding? What are the implications of not doing channel bindings with these attributes?"
    e. There is a valid reason to do this – e.f. FIPS-140 shop, someone comes in with WEP.
    f. Probably don't need the RF band based decision. Could be useful information to log.
    g. Limit some applications to 2.4 or 5GHz band.
    h. Didn't talk about which attributes need channel binding. Any RADIUS attribute could be sent in the channel binding. Would not make ciphersuite mandatory for channel bindings. Could list some attributes. Add text around this.
    i. 130 is the only remaining issue.
    j. May be an additional reason code.
    k. Minor editorial work remains; Bernard will post resolutions,
    l. IEEE 802.11 is meeting next week; additional comments may be provided.

4. Capability in RADIUS –Alan DeKok
    a. History
        i. Long discussions about capability in RADEXT
        ii. No real consensus, other than no consensus
        iii. This draft proposes something simpler than previous discussions
        iv. RADIUS has grown since those discussions
        v. capability is becoming more interesting
    b. Things to negotiate
        i. Can you do CoA?
        ii. Can you do packets longer than 4K?
        iii. Can you do extensions?
        iv. Can you do X?
    c. Representation
        i. Capability-Request packet
        ii. I can do X

  iii. Capability-Response packet
  iv. ACK we can do X
  v. Silent: we can't do X
  vi. These packets are link-local
  vii. are NEVER proxied
d. Some of these are end to end; from the point of view of the NAS, not my problem.
e. What is link-local? NAS and RADIUS server are client to server, never proxied.
f. Expect that first server encountered will respond.
g. Look at nai and answer for known further links?
h. Tag capability information per nai per realm.
i. Issues like 4K packet size mitigated by fragmentation draft. RADIUS accounting packets are 100bytes – need to use larger frames; local to NAS to RADIUS server link.
j. Capability Add
  i. 32-bit integer / enumerated value
  ii. specifies a well-defined capability
  iii. NOT "does RFC X"
  iv. Instead more "does RFC X section 3.2.1"
k. Capability Withdraw
  i. 32-bit integer / enumerate value
  ii. Counterpart to Capability-Add
  iii. Allows NAS to notify server that the capability no longer exists
l. IANA is place to register the capabilities.
m. Can shoe-horn capability definitions into specifications.
n. Motivation is from existing customer needs – particularly volumes of RADIUS accounting data on e.g. a gigabit link – with minimal changes to the existing infrastructure.
o. Don't we have the intention not to duplicate solutions – really have different protocols.
p. Currently an individual submission, not in the charter; get through current charter, then consider taking this up.
q. Poll – who else is willing to remind Alan to finish this document? And contribute and review? There are several co-authors at this point.
r. What happened 4 or 5 years ago, and what is different today? Thought at the time was to have more complicated capability definitions. Inside of existing attributes. Trying to include Diameter functionality into RADIUS. Didn't work. This is MUCH simpler – a few well defined capabilities.

5. Accounting via IPFIX – Alan DeKok presentation
a. The real problem
  i. Why is RADEXT defining what information should be used for accounting traffic flows?
  ii. RADIUS can transport data.
  iii. Defining "this is a traffic flow" is really outside of the scope of RADEXT
b. Benoit noted IPFIX: http://www.iana.org/assignments/ipfix/ipfix.xml
c. The benefit:
  i. We leverage the existing IPFIX registry
  ii. Can do flow-based accounting for **any** flow
  iii. MPLS, TCP , UDP, deltas, absolute counters, etc.
  iv. No need to re-invent the wheel
d. The drawback:
  i. IPFIX has 16-bit IDs

        ii. OK, a bit of work and we can hack them into RADIUS
        iii. Some other IPFIX things aren't relevant either
        iv. Security attributes, etc.
        v. probably 99% of the IPFIX attributes are relevant and useful in RADIUS
    e. Conclusion
        i. We should specify **transport**, not **content**
        ii. Once we publish a draft, the entire accounting problem will **go away**
        iii. Never to return
    f. The approach in addressing the use cases –TCP and UDP flows – is defined in IPFIX.
    g. IPFIX is evolving – if it adds new attributes, yes, need to revisit. If new attributes – no new work. Allocate one attribute from the extended attribute space and reference the IPFIX registry.
    h. Does Layer 2 (MAC address data type).
    i. Like this for one reason – don't reinvent the wheel. Agree.
    j. Steve H.:Have you talked to the IPFIX folks about this – not directly. Should do that – major IPFIX author (Benoit) is aware of this work. If move forward, specify mapping separately from the common RADIUS flows.

6. Support of fragmentation of RADIUS packets, draft-perez-radext-radius-fragmentation, Diego R. Lopez - Telefónica (diego@tid.es)
    a. Status
        i. -03 available since August
        ii. No objections received so far
        iii. Implementation work progressing
        iv. Request for WG adoption
        v. People to act as customary reviewers already contacted
    b. Implementation Goals
        i. Implement draft-perez-radext-radius-fragmentation
        ii. Serve as a proof of feasibility
        iii. Provide on-the-wire feedback for the specification
        iv. Proof of concept
        v. Intended for validating the fragmentation mechanism
        vi. Open source
        vii. Source code will be published once ready
    c. Implementation Details
        i. Based on FreeRadius 2.1.12
        ii. Client based on FreeRadius radeapclient
        iii. Scenarios to be implemented
        iv. Fragmentation of Access-Request
        v. Fragmentation of Access-Challenge
        vi. Fragmentation of Access-Accept
        vii. Will work through out-of-the-box FreeRadius proxies
        viii. No need of RADIUS fragmentation support on existing/deployed proxies
    d. Implementation Status
        i. Fragmentation of Access-Challenge
        ii. Completed
        iii. Fragmentation of Access-Request
        iv. To be completed in the next weeks
        v. Fragmentation of Access-Accept

vi. To be completed prior next IETF meeting

e. Chair: don’t see any reason this work can’t proceed to be an official working group item.

f. Plan to get reviewers, ask for them now.

7. Wrap-up

a. Next steps: work on re-chartering; publish charter update proposal in the next couple of weeks.

b. Comment on 4282bis – is this a WG item? Unchanged for 3 years. Believe we could move it out quickly.

c. Plan is to adopt it as a WG item in the re-chartering.

d. Have people looked at the document?

e. Need to review it carefully and get it out. Have an issue that other documents are not consistent with a document we haven’t written yet. Need to stop the documents.

f. Have documents saying that EAP methods use internationalization which don’t; are catastrophically wrong. proceed document has an issue.

g. How to solve it quickly. What is the latest proposal? Thought we agreed on all but accounting. Proposal is to leave off accounting and proceed with what was agreed.

h. Go fast with the new charter to solve 4282bis. If more urgent this – do an AD sponsor of the document. How much time will we gain?

i. Process is not the problem. Do need to review the document.

j. Benoit: Can go with the charter proposal, then 1 month for the document – goal is to be done with 4282bis in 2 months. If find that the re-chartering takes more time, then use another process. If this is urgent, AD will do his work, need WG to do theirs.

k. Conflicts between EAP and MSCHAP identity.

l. Benoit: can we accept this as a WG item right now? Any objection? No objection. Move it forward.

m. Benoit: MIB doctor requests – 5 directorates, why interest in MIB doctors, but not AAA? Will clean up list.

8. Meeting Adjourned 4:40pm