ACP update

draft-ietf-anima-autonomic-control-plane-28

Toerless Eckert tte+ietf@cs.fau.de (Futurewei USA)
Michael Behringer michael.h.behringer@gmail.com
Steinthor Bjarnason sbjarnason@arbor.net

v1.0
Status

- IETF 104:
  - draft-ietf-anima-autonomic-control-plane-24
  - Open Discuss Ben from Russ Housley about rfc822Name
- Received Joe Halpern RTG dir review
- -25
  - Remaining IPsec fixups with ipsecme mailing list (thanks Valery, Paul, Mcr, and other...)
  - Joe Halpern RTG dir review fixes
- -26 / -27
  - Fixes for Russ Housley on behalf of Ben Kaduk SEC-AD DISCUSS
  - Authors think all outstanding issues closed
- Responsible AD (Eric Vyncke) adds YES to IESG record
- ACP put onto IESG Telech at July (Barry Leiba)
  - Received new SEC AD DISCUSS/review from Roman Danyliv
  - Ben Kaduk tentatively cleared his DISCUSS
  - Barry Leiba delayed telechat for August 13. – too few Ads able to finish review (long document)
- -28 (IETF week)
  - Fixes for Roman Danyliv review
  - Authors think all outstanding issues are closed

(except complete typo run / work with RFC-editor)
-25 highlights / enhancements

IPsec:
Several minor good fixes, see changelog

Diagnostics request Mcr:
Want to make sure TA are signaled from both ACP peer sides even connection fails
Interesting logic needed with IPsec / CERTREQ option
Added text about how and why - example diagnostics (MTU office space diagnostics etc.)

Joe Halpern
Better explanation of unique use of Data-Plane
Data-plane =~ Data-plane in other documents for fully autonomic nodes (only control in ACP)
Data-plane =~ “all the router except ACP” for existing routers (non autonomic control plane part of data-plane)

Several RPL detail/text fixes

Better text for “ACP loopback”
Actually end up (IMHO) explaining why “loopback” is the right word (Eric was previously fan of new term)

Better text to justify zone addressing model
Incremental adoption model: ACP edges interconnected by non-autonomic core (e.g.: MPLS/VPN VRF)
Feedback from Russ, Ben why rfc822Name not to their liking was dragging on
Arguments changing when prior arguments refuted
Authors thought they had perfect explanation / justification in pre-version of -26

Toerless had call with Russ Housley, Barry Leiba
In hindsight should have been done earlier – email to mailing lists just does not work
Barry Leiba as responsible AD or 'email'
Thanks Russ, Barry for being available!

Alas, Barry of same opinion re. use of rfc822Name as Russ

Authors had to give up so as to not drag discussion along.
Maybe raise the concern independent of ACP in emailcore later
What is a valid rfc822Name ? (hopefully correctly re-stating positions)
Russ Housley: noreply@example.com can not have a certificate as I is not intended to receive email
Barry Leiba: MUST use primarily email / SMTP for an address to be valid email address

Now What ?
-26: rfc822Name change (2)

Proposal from Russ Housley
subjectAltName / otherName / <new>. Requires IANA allocations “around” <new>

Brainstorm alternative
subjectAltName / otherName / uniformResourceIdentifier
IANA alloc new URN: urn:ietf:params:acp:node:
Authors felt this would be better than <new>
No new type decoding required. Existing deparser would support it. Backend tools might support this field.

Final solution in -26
subjectAltName / otherName / AcpNodeName
Removes "rfcSELF:" prefix from rfc822Name string, keep rest same, changed encoding point into certificate
Coward approach: use what was suggested to authors. If it does not work, its not authors fault
Seemingly good experience with other solutions using this (hence recommended by Russ)
Can always define equivalent URN as add-on RFC.
-26 code tested by Russ (ASN.1 parser), allocations of code-points by IANA done.

Downside ? Vs. rfc822Name:
1. All the prior ACP versions listed technical downsides
2. rfc822Name would have allowed ACP registrars to use public CA that use:
   draft-ietf-acme-email-smime
   ACME draft much younger than ACP, so public CA never planned for ACP
   But would have been a great option for ACP now that it becomes available
-26/-27 other changes (Russ Housley review)

• Many good editorial enhancements on security text (Thanks Russ)!

• Highlight ?
  • Certificate key MUST requirements reduced to smallest reasonable sizes – 2048 RSA, P-256
-28 review / DISCUSS Roman Danyliv

- Many good editorial enhancements on security text (Thanks Roman)!
  - Several hopeful good additional explanations for readers in result.

- Highlight ?
  - Suggest learning clock insecure in absence of trusted clock info
    - Suggest to later learn trusted NTP across ACP (outside scope)
    - Could ignoring certificate time stamp create better results? BRSKI does this...?!
  - Refined text for attacks against impaired ACP nodes
    - ACP traffic can not be injected/extracted on impaired ACP node (admin access): requires at least support for non-autonomic option such as “ACP connect”
  - More elaboration about set of misconfigurations ACP protects against
    - Also re. “interface down” command (and maintaining ACP reachability across itnerface)
  - Actionable security consideration: “Operators must not make config mistakes”
    - But ACP reduceses significantly mistakes that will have them shoot in their own feet.

- Forgo MUST conform to RFC8247 (when doing IPsec).
Thank You!

ACP will return