ACP update

draft-ietf-anima-autonomic-control-plane-30

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

v1.0
-29 – The final edit

• Converted to XMLv3 to get new XML tags to use for contributor
  • Moved Pascal (RPL), Michael (BRISKI, RPL), Brian (GRASP) from ack. to contributor
  • XMLv3’ification should also speed up RFC editor pass - RECOMMENDED (Brian also did this for GRASP to help RFC editor)

• Closed all remaining “DISCUSS” from IESG – Roman Danyliv, Ben Kaduk, Barry Leiba
  • Not sure if those qualified for DISCUSS, but would have been all good comments anyhow.

• Closed all COMMENTS from IESG

• Highlights
  • Ca. 2 additional pages node security considerations, including
    • IDevID/LDevID needs to be protected from private key extraction (TPM or the like), secure boot/software, etc..
    • EST / Registrar security considerations, constraining certs with id-kp-cmcRA to better protected devices (physical device security) to prohibit impairment of registrars == impairment of domain (aka: registrars are critical infra)
    • Impaired non-registrar ACP node (man-in-middle) can not create new functional attacks other than filtering traffic (wrt. e.g.: GRASP discovery of EST server announcements)
  • Signaling of non-well-known-port number via DULL GRASP is another attack vector
    • Attacker on LAN can send e.g.: ACP over DTLS with 10,000 port numbers (DoS attack)
    • But “experts” not willing to agree that using well-known port numbers would be a good way to overcome issue. Toerless picked wrong experts to ask (mDNS: same problem, but their “services” very much depend on not having to assign well-known port numbers, whereas ACP-over-DTLS would be a very reasonable future ask (except that maybe now QUIC will superceed DTLS....)
  • Finally got the extension point syntax for AcpNodeName and GRASP right...
  • New separate section for “TLS security requirements” (6.1)
    • Merged from other places. Finally the short section other similar RFCs could steal (5 years ago GRASP ? ;-) 
  • New A.10.9 for possible future ASA “discovery ACP secure channel downgrade attacks”

• Aka this all took time because there was a lot of fine-tuning of security text details involved
  • But security folks from IESG seem to like the result now
The leftovers

- Final pass with Eric Vyncke (ACP responsible AD)
- Toerless’ “denglish” vs. Microsoft spell checker: 0:100, microsoft wins.
  - Really didn’t make sense to attempt repeating this for every prior draft version because i did not find a way to avoid the 1000 non-issues raised (recurring wasted time)
- Four considerations where we could not get agreement and/or enough review, so can not be in RFC
  1. Making secure channel negotiation better / safe against downgrade attacks via an initial TLS/GRASP negotiation step
     - Was marked for removal in RFC for years now already, as WG thought it was too complex. Ben Kaduk actually likes the idea and also contributed text, but of course, e-too-late now for RFC
  2. New: answer to Q: from BenK “should ACP address of peers certificate be verified at transport stack” – IMHO NO, does not make sense, but not enough time to discuss this
  3. Recent (since ca -25) How would ACP work with Public CA? Some IMHO good and correct text, but Mcr started to also have interesting (counter?)arguments...
     - Hint: if we had been able to keep rfc822Name, we could be using public CA NOW for ACP... *sigh*
     - So... Having this argument/text in a future draft might be a lot better to continu this line of thought
  4. Hardening DULL GRASP (from -29)
- These four considerations now in new appendix B.
  - Marked for RFC editor removal
  - Toerless tried to innovate a new way to leave breadcrumbs in the RFC to these leftovers –reference to [ACPdraft], but Eric couldn’t bring himself to approve of this
  - Aka: “normal” IETF process “you need to know” – look into last draft to know what didn’t make it into the RFC.
Cluster C325 unlocked pending RFC-edit work (top of queue ?!) Thank You!