An Autonomic Control Plane

draft-ietf-anima-autonomic-control-plane-05 (ietf98:06 - ietf99:08)

99th IETF, July 2017

Michael Behringer (editor), Toerless Eckert (editor),
Steinthor Bjarnasson

06-07:

- GRASP objective indicates set of channel protocols it support
  - ACP peers can try only the protocols they mutually support

- Expanded “ACP connect” section explaining how it works:

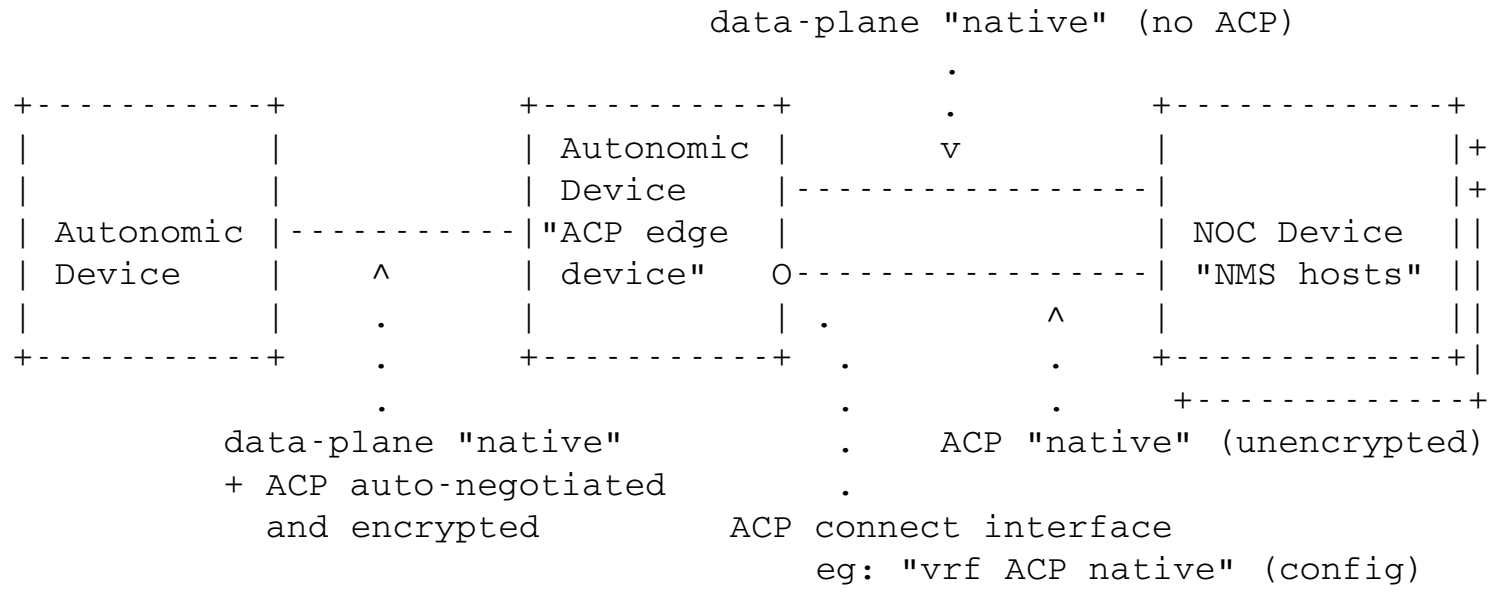

Figure 6: ACP connect

06-07:

- Moved GRASP via TLS negotiation of ACP channel into informative section at end (“future work”). Rewrote to relate to IKEv2
  - Should propose via separate spec
  - Need to specify actual GRASP negotation steps. Need to compare/be better than IKEv2 negotation to make sense.
  - Still tink this is viable when trying to negotiate into currently non IKEv2 supported options like 802.1ae. Can not imagine that those alternatives could realistically be supported via extensions of IKEv2:
    - Even if we get the standard extended, who would risk modifying a crucial crypto implementation (IKEv2) on core network devices for this…
  - Removed IANA allocation requests corresponding to GRASP/TLS

06-07:

- ACP information field: name for ACP stuff in cert.
- Rely on domain in ACP information field instead of OU to mutually authenticate certs.
  - Make certs easier re-useable. Do not depend on fields other apps may want to use differently (we do not own OU field).
  - Text also mandated that through extensions one would be able to auth certs from other domains -> would never be able to predict what their OU are.
- Made ACP information field extensible (see slide for -08)

06-07:

- ACP neighbor discovery via GRASP from ani-objectives draft
  - Detailled test explanation of fields as well
  - Included full message format to show locator as well (must be same as session-id).

```
[M_FLOOD, 12340815, h'fe8000000000000c0011001FEEF0000, 1,
            ["AN_ACP", SYNCH-FLAG, 1, "IKEv2"],
            [O_IPv6_LOCATOR,
                h'fe8000000000000c0011001FEEF0000, UDP, 15000]
          ]
```

The formal CDDL definition is:

```
flood-message = [M_FLOOD, session-id, initiator, ttl,
                 +[objective, (locator-option / [])]]

objective = ["AN_ACP", objective-flags, loop-count,
                                        objective-value]

objective-flags = ; as in the GRASP specification
loop-count = 1    ; limit to link-local operation
objective-value = text ; name of the (list of) secure
                       ; channel negotiation protocol(s)
```

06-07:

- Only protocols are not IKEv2 and dTLS
  - IKEv2 itself negotiates native vs. GRE encap
- No need for any port assignment for dTLS
  - Port on which dTLS tunnel runs is announced in GRASP

07-08:

- 08 posted today
- Full run through document, goal:
  - Code complete
  - -> shepherd review -> WGLC

- Terminology section
- Normative / Informative section
- Tried to resolve all Ednotes and other open items
- Marked all major sections as Normative / Informative
- Move sections that was side-notes/extensions further down
  - Hopefully lot easier readable structure
- Fixed limited number of functional aspects that where wrong

07-08:

07-08:

07-08:

- Domain Certificate handling
  - Make BRSKI optional (not normative) reference for ACP
    - ANIMA modularity: allow reuse of ACP, BRSK, GRASP individually
    - Provides clarity that real precondition is only the magic cert with ACP info.
    - Allow variants with eg: netconf zerotouch boot.
    - Informative section explains BRSKI benefits (as developed in last months in BRSKI)
      - Short-lived cert simplicity (no CRL needed), re-enroll instead of renew after expiry!
  - Now EST is mandatory reference in ACP
    - And Certificate maintenance section describes GRASP objective for EST server and MUST have EST servers (for cert renewal)
    - Why ? BRSKI text evolved over last year to focus only on bootstrap extensions.
    - Cleaner to refer directly to what we want from EST for renewal than to refer to BRSKI which does not really care about non-bootstrap parts of EST.
  - ANI devices MUST support BRSKI and ACP
    - Have to decide where to say this normatively. BRSKI ?
    - Can not say in reference model (informative).

07-08:

- Cert maintenance – more details:
  - EST server ACP address provisioned during domain cert provision/enrollment, but can also be learned via GRASP M_FLOOD announcement.
  - M_FLOOD “closest by” EST server preferred, Fallback to provisioned/configured server (explaining with attack by compromised ACP member).
  - MUST support domain certs with HTTPs CDPs with with ACP address for revocation. Just in case BRSKI is not used or short-lived cert option is not desired.
  - Renew after 50% lifetime expiry for reliable problem resolution.
  - Not sure what more details on Cert parameter/mainentance are required to pass IESG SEC AD review… will see.

07-08:

- Problems:
  - Text about domains / subdomains was suggestive in a way that it was unclear how to build future extensions.
  - Was impossible to have different ULA prefixes inside same domain. Would require Intent to be defined to use multiple ULA. Multiple ULA would be good for aggregation, but depending on Intent to be done may be risky.
  - 0x-07 said: „just cross-sign certs from different domain so ACP can be built across domains – just cross-sign Certs“
    - This would NOT have worked in <= 07 due to OU checking
    - Also: cross-sign certs expensive operation
  - OU checking when building ACP also would make it more difficult to add ACP information to just „any“ certs that can be reused in other services on the devices.
  - Asks how we would be able to support alternative routing protocols.
  - Rfc822 encoding had problems.

07-08:

- ACP information in cert ACP information field:

  anima.acp+<acp-address> {+<rsub>{+<extensions>}}@<domain>

  anima.acp+fda379A6f6ee0000200000064000001+area51.research@example.com

  Domain = example.com

  Routing Subdomain = <sub>.<domain> = area51.research.example.com

- *Not using RFC5952 for acp address, „:“ is not permitted in simple local-parts.*

- Domain part must be same for ACP to be built (no OU anymore!)
- Routing subdomain is used to create address:
  - hash(routing subdomain) = /40 ULA prefix
  - rsub optional: normally routing subdomain == domain
  - Only use multiple routing subdomains when you know what you want to do

07-08:

- Domain, subdomains, CA – clarified how they interact:

- Routing subdomain cheapest way of subdomains without additional intent.
- Eg: extend with GRASP negotiation.
  - Could add different routing protocols to different subdomains.
  - Or jst negotiate how to do aggregation across routing subdomains.

- Do not mutually cross-sign certs, but if different domains should form ACP in future, add othrer sides CA as additional trust anchors.

07-08:

- ACP neighbor discovery:
  - Moved L2 discussion and CDP/LLDP/mDNS discussion out of the section (explain later in these slides) to keep the core part of the document focussed on describing only necessary text but not optional choices or decision making considerations.

  - Added text about bringing up of interfaces to discover ACP neighbors.
  - Added text to explain how ACP/BRSKI time-share DULL GRASP instance (unenrolled: BRSKI, enrolled: ACP).

07-08:

- Added Michael R's proposed addressing scheme with 256 virtual addresses (V8 addressing) as equal option to Zone addressing.
- Reworked with Pascal Thubert RPL profile to match Michael Richardson template
  - Michael: Get that draft out, we can not build an xref to an expired draft ?!

- Explained RPL single instance pro/cons
  - Pro: No dataplance artefacts
  - Cons: No shortest paths to multiple NOCs
  - Can expand RPL profile through later work

07-08:

- GRASP in the ACP:
  - Defined GRASP in ACP as mandatory part of ACP services. Explained how this is primarily about service (objective) discovery across ACP as mandatory requirement for zero-touch self-organiation of ASA. Moved L2 discussion and CDP/LLDP/mDNS discussion out of the section (explain later in these slides) to keep the core part of the document focussed on describing only necessary text but not optional choices or decision making considerations.
  - Defined ACP as “transport and security substrate” for GRASP
    - Terminology introduced into GRASP spec during IESG review.
    - Aka: ACP provides authenticated and encrypted communication environment within a trusted group.
  - Mandate TLS 1.2 for GRASP unicast. Explained why:
    - Attack vector of compromised ACP devices performing man-in-the-middle-attack
    - Change from prior requirement to only use TCP (but ACP secure tunnels only protect from the outside).

07-08:

- Discussion of L2 switched LANs and ACP support:
  - 00-07: up early in “precondition” section, threw in a lot of L2 stuff early in the document. Was only there to justify selection of DULL GRASP over mDNS. Derailing & incomplete.
  - 08: moved as “ACP on L2 switches/ports” directly before “Workarounds” (ACP connect, ACP tunnels). Expanded text:
  - Now instructive enough to allow and request (“SHOULD”) support for per-L2 ACP support on L2/L3 devices.
    - Why: large L2 LANs (eg: broadband aggregation, enterprise, IoT).
  - Details explained eg:: how to do DULL GRASP per L2 port.
  - Comparison of DULL GRASP vs. mDNS even later in document, so the logical order is maintained.

07-08:

- Moved appendices before security/ANA considerations
  - Section “Further Considerations (Informative)
    - Reviewers raised concerns of appendices not being read.
- Consideration: “Domain Certificate provisioning / enrollment”
  - As explained in before in this slide deck
- Consideration: Why ACP routing via RPL (unchanged)
- Consideration: ACP secure channel negotiation via GRASP/TLS
  - Was normative in 07. Made information ”to be investigated option” in 08
  - IKEv2 claims to be generic negotiation protocol (MichaelR), So why GRASP/TLS
  - IMHO: unlikely successful / expedient in in defining IKEv2 negotiation extensions to include eg: selection of dTLS or 802.1ae or other secure channel protocols (see KARP experience).
  - BUT: We can not keep GRASP/TLS text in normative section because it was just inspirational but not descriptive, eg: no spec of the actual negotiaion GRSP messages defined.
    - Requires followup work. Requires more evidence of interest in that work.
    - Considerations section now discusses also IKEv2 and states that a future proposed GRASP/TLS soluton would need to measure up to IKEv2. Example of performance (HW/SW) based selection given as key candidate requirement.

07-08:

- Separated references into normative/informative
  - BRSKI is informative !

07-08:

- Self-Protection properties:
  - Added explanation that ACP security is meant to protect legacy non-secured management protocols as a STOPGAP.
  - Added subsection for attacks from the inside
  - Described that traffic inside ACP SHOULD use end-to-end encryption whenever feasible (and done by ANIMA defined/used protocols), that the domain certificate can used for this and that ACP is primarily about realiable connectivity.
  - Added notion that devices with domain certificate need to be secure so they can not easily become comprimised insiders.
  - Added notion that future extensions such as assigning roles to domain certificates could help to further mitigate the impact of attacks from the inside.

Next steps

- Close what we can in Chicago
- Candidate last call version before next IETF.