Bootstrapping Key Infrastructures

Max Pritikin

IETF 96, 18 Jul 2016

v_02

Topics

Current document EDNOTEs include:

- Current Proxy Model (text has changed here, would like awareness)
- Possible CoAP alignment (in scope? out of scope?)
- Possible MUD alignment (decision on preferred method)
- Rogue Registrar Mitigation methods (limitation in current model. Suggested improvements?)
- CMS vs JWS (justify current choice, solicit feedback)
- Anima specific cert fields (not a bootstrap specific issue: can be covered in ACP draft?)

Proxy (and discovery)

- s3.1.1 New Entity discovers Proxy

  New Entity MUST mDNS

  Use case: mDNS already assumed by most IoT. (e.g. lightswitch w/o anima)

  suggested: Proxy “MUST be discoverable using insecure GRASP”

  implies “New Entity [MAY | SHOULD | if/MUST] insecure GRASP”

  This is confusing: The normative language for NewEntity and Proxy differ?

- s3.2.1 Proxy discovers Registrar

  “The address and port of the Registrar will be discovered by the GRASP protocol inside the ACP”

  suggested: Registrar “MUST be discoverable using (secure) GRASP”

  Registrar is “configured or SHOULD be discovered using GRASP for autonomic installations”

- GRASP document to be updated with details on “insecure GRASP”

Circuit proxy

- “MUST implement an IPIP (protocol 41) encapsulation function for CoAP traffic”
- “SHOULD also provide one of: an IPIP encapsulation of HTTP traffic on TCP port TBD to the registrar, an HTTP proxy which accepts URLs that reach the Registrar, or a TCP circuit proxy that connects the New Node to the Registrar”

  (These choices are between the Proxy and Registrar, and are transparent to the New Entity. The exact mechanism could be determined by the GRASP exchange)
- The proxy<-Registrar channel is intended to be over ACP. There is no normative text about this.

CoAP

- CoAP

bootstrapping is expected to be important to a large class of devices that run CoAP. Even if we declare this out-of-scope we need to understand the interactions

s5.7.5 but to be promoted to s5.8 as its BRSKIoCoAP

- Initial thoughts captured in: draft-pritikin-coap-bootstrap-00

based on draft-ietf-core-block-20, multiple REST payloads to xfer the body of the message.

- Object Security for CoAP (OSCOAP)?

section4 points to COSE and “render more compact objects”, but not generic support for fragmentation

This might not be sufficient when dealing with certs.

Registrar contacts MASA

- s3.3.3 Claiming a New Entity by contacting…

  Manufacturing Authorized Signing Authority

  Vendor Service, etc

- **Given a device from an arbitrary manufacturer how to distribute the URL of the MASA?**

  [[EDNOTE: An appropriate extension for indicating the Vendor URI and imprint method could be defined using the methods described in [I-D.lear-mud-framework]]]

Privacy Preservation

ie. without giving up the device identity to observers on the network

Current TLS prevents passive monitoring. TLS 1.3 expected to protect against active as well.

s5.2 Request Audit Token from Masa

- Threat:

  The Registrar is an unknown entity to MASA . It might be attacking the system.

  Example: Rogue Registrar(s) could DDoS attack the system by claiming devices it does not possess

- Existing Mitigations:

  Registrar authentication & sales channel integration (MASA knows who owns which device)

  nonce checks and log consolidation

- **Should we add optional proof-of-possession?**

e.g. server MAY require extra round trip in s5.1 and 5.2 and this of course doesn't work in offline case

s5.3 Audit Token Response

- Current text:

  “The [JSON] audit token response is encapsulated in a [CMS] signed by the MASA server. The New Entity verifies [with] manufacturer installed trust anchor.”

- This is consistent with CMC
- But:
  - EST allows client to avoid fullCMC parsing
  - Attempts are made to ensure “certificate-less” can be defined)

- Alternatives: JSON Web Signature?

How does BRSKI conclude?

- Rolls into certificate enrollment for efficiency
  - s5.3.1 “the New Entity SHOULD use the existing TLS connection to proceed with EST enrollment, thus reducing the total amount of cryptographic and round trip operations required”
  - (This is a clear transition point to support certificate-less deployments)

- Once BRSKI has distributed trust anchor New Entity we have no normative statement about what is next

s5.7 post-BRSKI EST

- s5.7.1 CA certs
  proper distribution of entire chain (a la CMP)

- s5.7.2 mandates CSR Attributes
  next slide

- s5.7.3 basic enrollment

- s5.7.4 enroll status telemetry
  new concept

s5.7.2 CSR Attributes

- Why does this exist?

  “inform the New Entity of the proper fields to include in the generated CSR.”

  Intended for fields unknown to infrastructure like MAC address

- Anima interactions

  Details of cert fields belongs in ACP (s5.1.1)

  GRASP discovery implies RFC6125 style SRV-ID or similar?

- These could be communicated to New Entity via CSR Attributes?

  The Registrar can only override New Node CSR using fullCMC or CMP.

  Some backend PKIs or not standards compliant.

  Ensuring correct CSR is in Anima’s interests

Next Steps

- Follow up on netconf ‘ownership voucher’ integration as previously discussed

- What are we missing that you care about? Engage authors and let us know. Join calls.

- Finish PoC implementations