ANIMA
BRSKI

Bootstrapping Remote Secure Key Infrastructure

For 6tisch WG
And netconf
And ANIMA

Michael Richardson
mcr+ietf@sandelman.ca

https://www.sandelman.ca/SSW/ietf/meeting/ietf101/ietf101_anima_brski_homenet

What is ANIMA?

802.1x/EAP/PANA has this “solved” for initialized nodes which know which network they want to join; need to be pre-provisioned with certificates.

- needs EAP-TLS to make this work, which then includes new layers of fragmentation. This code is used once!
- PANA/1x authenticator function scales with number of nodes attempting to join, is subject to DoS attack, defending against may be too expensive for constrained nodes
- 1x function for ANIMA **ACP** bootstrap may interfere with 1x function being provided by routers/switches for end-hosts!

Autonomic Control Plane

How to bootstrap trust?

Join (Enroll) Problem

How to securely let new devices into a network without destroying the network.

- The goal is to provision new nodes with certificates, at which point “traditional” methods may be used to secure network (802.1x/EAP)
- Nodes are uninitialized
- They are “drop shipped” directly from the warehouse.

Things Homenet does not need

- ACP is overkill
  - Just use BRSKI
- Intent-based policy
  - But ANIMA hasn’t got it anyway, and SUPA is dead.
- Maybe even PK*I* is unnecessary
  - Just use secure transport to exchange PSKs, or exchange RPK.

Things HOMENET probably wants

- Integration of BRSKI + MUD.
- Manufacturer involvement
- “push-button” extensions (see appendix) to BRSKI to operate with reduced security.

Challenges for HOMENET

- Unmanaged network --- no infrastructure!
- Who/what will run the JRC?
  - Is there any PKI?
  - If so, what happens when the PKI machine is replaced?
    - Perhaps, quite abruptly.
    - His/Her JRCs?
- Interactions with “SmartHome”, etc. IoT things.
  - Having BRSKI would be good.
  - Maybe IoT network will provide JRC?
- What is the fallback when there is no JRC?
  - Chicken and egg situation
- Can the JRC be cloud-located?
  - Can it be outsourced?

Layer-8 and layer-9 issues

- Relates to entire HOMENET challenge: who is gonna pay for ongoing maintenance?
  - Does the end-user want to be beholden to that entity?
- Is there a fax-effect we are missing?
  - Can providing HOMENET security enable other things?

While often an IETF tradition to claim this is out of scope, too many of our good ideas die because we did not figure how the incentives would work

If the home user is in fact the “product” for another entity, we might want to think hard about privacy issues sooner.

Some additional thoughts/hopes
http://hubofallthings.org/

- Aims to be a place to keep one's personal data, self-owned.
- Seems an obvious place for a JRC function!
- Currently cloud-based, for pragmatic reasons.

My experimental JRC/hubofallthings

How to proceed - 1

- Finish current work!
- Help ANIMA and 6tisch review our current documents.
  - Are there MUST NOTs that you think would have to change for Homenet?
  - SHOULDs which HOMENET can not do, likely are less of a problem.

How to proceed – 2 - profile

- Write a profile of BRSKI for HOMENET.
  - Do you want full BRSKI (HTTPS, JSON format vouchers + CMS signatures)
  - Or constrained voucher (CoAP +{DTLS,EDHOC}, CBOR format vouchers, COSE signatures)
  - May have to support both to enable the “home office” to use enterprise equipment, while still speaking to IoT.
  - What kind of join proxy will you make MTI?
    - BRSKI default is stateful, but trivial to code, constrained default is stateless, but a bit harder to code.

How to proceed – 3 – Legacy/fallback considerations

- Figure out what a BRSKI-HOME device will do in a legacy home.
  - Probably call home with NETCONF zero-touch!
    - Hope this does not lead to still-born protocol!

Questions/Discussion

?

Michael Richardson
mcr+ietf@sandelman.ca

https://www.sandelman.ca/SSW/ietf/meeting/ietf101/ietf101_anima_brski_homenet

How to proceed – 4
find cool acronym (an IETF tradition)

- Find a way to expand the acronym "RADLER" (which is a nice summer beer with grapefruit juice)
  - Remote ADder for Lots of Exciting Routers