BRSKI document status for IETF104, Prague. March 26, 2019

Authors:

Max Pritikin,

Michael Richardson

and

Kent Watsen

BRSKI document – passed WGLC

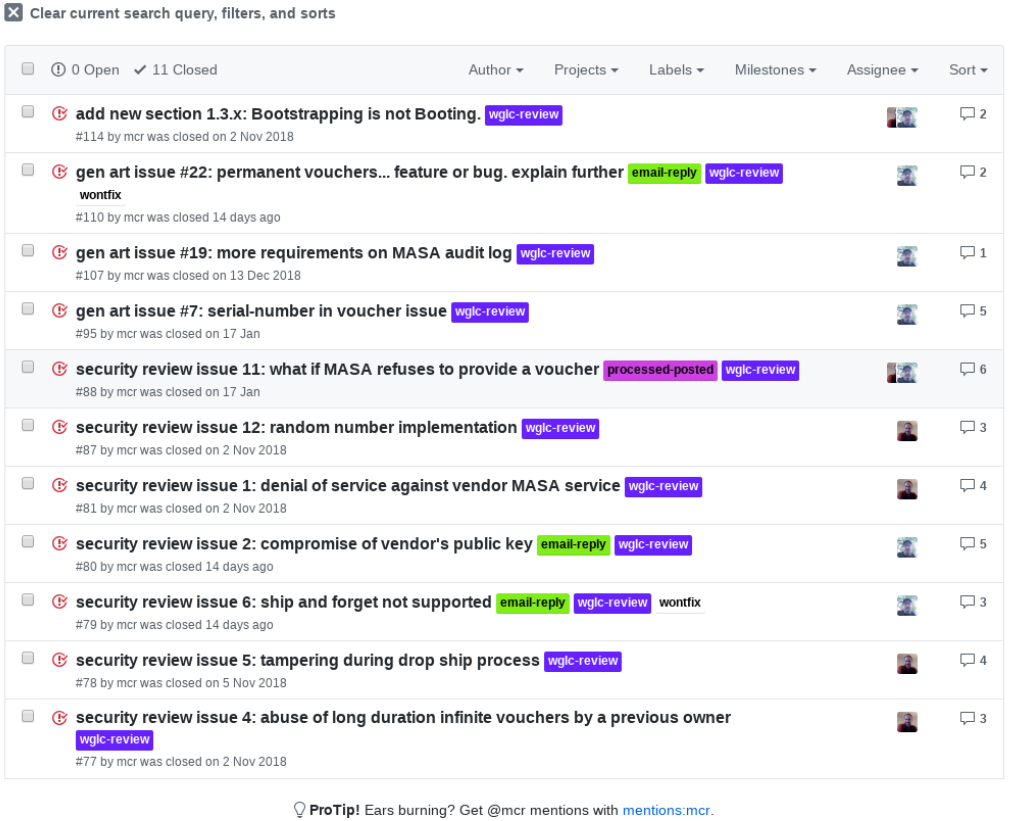
- Received Three reviews:
  - GenART review from Jari Arkko, see it here:
    - https://www.ietf.org/mail-archive/web/anima/current/msg03866.html
    - https://mailarchive.ietf.org/arch/msg/anima/iVg7MRMdBQBVFA5VFiksYFHchBU
  - SecDir review from Christian Huitema, see it here:
    - https://mailarchive.ietf.org/arch/msg/anima/XCS6JpwQSm3naOivwCYaO0AAsVs
  - IoT Directorate review from Russ Housley
    - https://mailarchive.ietf.org/arch/msg/anima/1N7AR8hqu2oIWuTFFd9OQOab8S
- Posted version -18 and -19 with incremental improvements, summary of final activities posted to mailing list
  - https://mailarchive.ietf.org/arch/msg/anima/Sjr2Yy1YNfUw3WVv1EqOa7Swef0

Github Issues on BRSKI

- https://github.com/anima-wg/anima-bootstrap/issues?utf8=%E2%9C%93&q=is%3Aissue+

- Many improvements to text, added a number of sections:
  - (1) new section 5.3: Registrar Authorization of Pledge
  - (2) new section 3.1: Nonceless Voucher Requests
  - (3) new section 8: Applicability to the Autonomic Control Plane (plus other details in the document)
  - (4) new section 9: Privacy Considerations:

- Tried to narrow scope to ANI needs, lest ocean boiled.



Interop testing of BRSKI

BRSKI-19
Contains many clarifications

- Being adopted by Thread Group
  - For details ask them.
- DOTS wants to use it

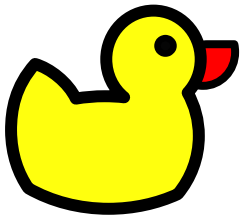
- In active Interoperability testing by FairHair Alliance
  - Third in-person session occuring Monday and Today.
- In use by CIRALabs SecureHomeGateway

- Client (pledge) implementations from :
  - NXP, Silabs,
  - Signify, Cisco
  - Sandelman, Siemens (test client)
  - ZHAW

- MASA / Registrar implementations from:
  - Siemens
  - minerva.sandelman.ca

Some BRSKI iconology

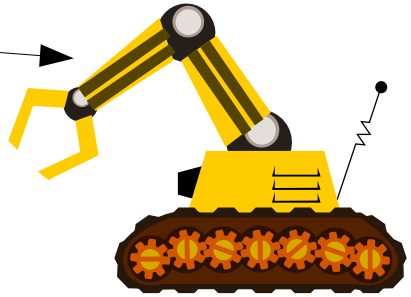
- Pledge



Stajano, F. and Ross Anderson,
"The resurrecting duckling: security issues for ad-hoc wireless networks", 1999,
https://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf
Wikipedia, "Wikipedia article: Imprinting", July 2015,
https://en.wikipedia.org/wiki/Imprinting_(psychology)
https://en.wikipedia.org/wiki/Animal_House

- Join Registrar/Coordinator
  - JRC
  - Registrar

- Manufacturer Authorized Signing Authority -> MASA.



- VOUCHER
  - RFC8366

Major Issue for WG

- Should we completely remove unsigned pledge voucher request?
  - Offline case has **no** voucher request from pledge, and in the online case it seems to offer only illusion of security, with no significant reduction in crypto for pledge.
  - Was written as a compromise for limited devices, but constrained-voucher seems to be better fit.
- Corollory, should constrained-voucher include unsigned voucher requests? Always? Never?

Document now with AD/IESG
Questions?

?