Babel Security in Homenet

Barbara Stark

AT&T

What babel WG will likely deliver

- Babel WG is currently working towards 2 solutions: HMAC-based and DTLS. Different use cases have different requirements, so both are likely to proceed.
- Summary of tradeoffs:
  - HMAC is simple, secure, and has few features (symmetric keying, small number of simultaneous keys per link);
  - DTLS has all the features of DTLS, but depends on DTLS, which is a more complex stack.
- Drafts (there are currently 2 HMAC drafts – babel is expected to pick one):
  - https://datatracker.ietf.org/doc/draft-decimo-babel-dtls/
  - https://datatracker.ietf.org/doc/draft-do-babel-hmac/
  - https://datatracker.ietf.org/doc/draft-ovsienko-babel-rfc7298bis/

Points I’m supposed to convey

- Babel WG is expected to recommend one security mechanism for all Babel implementations.
- Independent of (but informed by) that recommendation, homenet should choose what makes sense as MTI in a homenet "use case" context.
- Homenet should also decide if any optional-to-implement features are MTI for homenet.
- Homenet needs to define how keys/credentials get distributed in a homenet context (distributed by HNCP? by a new protocol?).