BPSec Update

Edward J. Birrane, Ph.D.
Edward.Birrane@jhuapl.edu
443-778-7423

APL
JOHNS HOPKINS UNIVERSITY
Applied Physics Laboratory

Status

- SBSP adopted by DTNWG and renamed BPSEC
  - https://tools.ietf.org/html/draft-ietf-dtn-bpsec-00

- Changes under discussion today:
  - Remove BAB
  - Remove Security Destinations

- Supporting Docs
  - Security Practices
    - *https://tools.ietf.org/html/draft-birrane-dtn-sec-practices-00*
  - Suite B Profile/Ciphersuites
    - *https://tools.ietf.org/html/draft-birrane-dtn-bpsec-suiteb-profile-00*
    - *https://tools.ietf.org/html/draft-birrane-dtn-bpsec-suiteb-ciphersuites-00*

Change 1: Remove BAB

Can we assert hop-by-hop authentication w/o BAB?

- Last Meeting Agreement:
  - Agreement to remove BAB
  - Security Practices Document captures ways to achieve hop-by-hop authentication
- Three Ways
  - (1) Always use authenticating Link Layers
    - *No extra mechanism at the BP layer necessary*
  - (2) Ephemeral Block Integrity
    - *Sign some existing block in the bundle, such as the PHN*
  - (3) Make user block with some bundle-wide signature
    - *Make sure bundle has arrived without a particular change (addition/removal of blocks.*
    - *Necessary to catch modification of block between BPAs when not using authenticating link layers.*

Change 2: Remove Security Destinations

Security destinations no longer useful and perhaps confusing

- Security destinations == bundle destination
  - Force all security processing at destination
  - What about items like integrity on an ephemeral block?

- Proposal
  - Remove security destinations.
    - *Security blocks are handled at a receiving node as a matter of policy for the receiving node.*
    - *Bundle destinations MUST process security blocks in the bundle.*
    - *However, so can waypoint nodes, if more appropriate.*
  - Security operation, target block type, and security source node sufficient to determine how to handle a security block at each node.