Status of HIP Related Internet Drafts

TMRID Interim Meeting
Feb 6, 2020
Robert Moskowitz

HIP Related Drafts to date

- Draft-moskowitz-orchid-cshake-00
- Draft-moskowitz-hip-new-crypto-04
- Draft-moskowtiz-hip-hierarchical-hit-03
- Draft-moskowtiz-hip-hhit-registeries-01

Draft-moskowitz-orchid-cshake-00

- IETF106 TMRID BOF consensus that ORCHID changes buried in other drafts need its own draft
  - This is an update to RFC 3743, not 7401
- Minor updates ready to be submitted

Draft-moskowitz-hip-new-crypto-04

- Removal of ORCHID content
- Changes in KEYMAT process
  - Result of extensive discussions with NIST and KECCAK Team
    - Physical meetings, not just emails and calls
  - Working with Keccak Team for comments to NIST to update SP800-56Cr1 to reflect discussions

Draft-moskowtiz-hip-hierarchical-hit-03

- Removed ORCHID related text
- Changes to DNS interaction
- Some other nits

Draft-moskowtiz-hip-hhit-registeries-01

- No updates since IETF 106
- Minor nits ready to submit
  - Including change to xml2rfc v3
    - All drafts at v3 now

Possible additional work

- We need a draft from IPsecme
  - Update IANA for EDDSA
    - We use this in HIP DNS RR
- ESP KMAC Transform draft
  - Not strictly (yet) for TMRID
  - Wait for NIST Lightweight crypto for new AEAD as well?
    - Or maybe get the draft in place and add later

Questions?