DRIP UAS RID

draft-ietf-drip-rid-03.txt
October 28, 2020
Robert Moskowitz
Etal.

Exhausting Review of Updates and brief todo
Updates

• Fixed some typos and awkward syntax
• Explicitly call out that HHITs are IPv6 addresses
• Section on non transferability of HHITs
• Expanded Remote ID Authentication section
  – Replaced reference to drip-auth with Appendix E examples
    • Self-Claim (84 bytes) and Offline-Self-Claim (200 bytes)
Updates

• Security Concerns
  - HHIT Trust
    • Replaced reference to drip-auth with sec 3.4 which points to Appendix E
  - Cleaned up Collision Risk section
Updates to Appendix B HHITs

- Expanded text on Prefix
- Added support for 8 bit Suite ID
  - This is to enable HDA domain Suite IDs
    - Should we really do this?
    - No provision for HDA HI algorithms.
      - Don’t know how. Yet.
Updates to Appendix C ORCHIDs

• Is this still an addendum to ORCHIDv2, or v3?
  – If v3 can it be buried in drip-rid or its own document

• Changed field order!
  – Prefix | RAA | HDA | HIT Suite ID | HI Hash
  – This is important, and I believe this is the correct order
Updates to Appendix C ORCHIDs

- Fully parameterized length of all fields
  - Prefix MUST be 28 or less
  - But if Info == HID, it is always 32
  - OGA ID can only be 4 or 8

- ORCHID Encoding
  - Added Context ID value (left out)
  - Added fixed hash length support as in ORCHIDv2
Updates to Appendix C

ORCHIDs

• ORCHID Encoding (more)
  - Added text for HIT per 7401 Encoding
    • Backwards compatibility of coding

• ORCHID Decoding
  - Added text for HIT per 7401 Decoding
Updates to Appendix D

- Fixed error in length of cSHAKE128 output to specify variable
  - Bad copying from source
Updates to Appendix E
HHIT Self Claim Examples

• These are EXAMPLES

• Addressed replay attack of old version
  - My bad, did not follow my original design for them

• How do we balance replay attack window against computing cost?
  - This is for real Self Claims in drip-auth!
  - There are a number of migrations possible there
Updates to Appendix E

HHIT Self Claim Examples

• **Added Offline Self Claim**
  - PLEASE note how it is necessary to ‘turn this inside out’ to address replay attack
  - Included text for generation
  - Included text on HDA HHIT|HI cache for Observer to validate claim
Updates to Appendix F

- Added table for Collision Risk based on hash size.
Still to do

- Still references other drafts
  - draft-moskowitz-crowd-source-rid
  - draft-moskowitz-secure-nrid-c2
  - Should changes be made to remove these dependencies?

- I think that is it!
Call for WGLC!
QUESTIONS?