Adding Hierarchical HIT Support to HIPv2

draft-moskowitz-hip-hierarchical-hit-01
IETF 106 TM-RID BOF
Nov 19, 2019
Robert Moskowitz

Why Hierarchical HITs (HHIT)?

- Implicit domain of use
  - The hierarchy information informs what the HIT is for
- HHIT associated with hierarchy
  - Duplicate prevention
  - Defense against HIT hashing attacks
- Scaleable lookups

Why Hierarchical HITs Now?

UAS Application

- UAS could use National Domains
  - FAA (and other CAAs) provide RAA services
    - These are minimal, to registering and signing HDA HHITs
  - Regional UTM provide HDA services
    - Connected to their UTM services
- UA flying from Canada to US would be quickly identified as such
  - Or maybe just launched in US

UAS Application

- Each CAA can apply its own policy on its UTMs and any other HHIT HDA providers.
  - And still support International usage of UA
  - UA free to register with unique HHIT for each region it operates in

HHIT design compromises

- Stay with the HIPv2 HIT design
  - 96 bits for hierarchy and HI hash
- 64 bits adequate for HI hash
  - 0.01% collision risk in population of 66M
  - 1% collision risk in population of 663M
  - Collision prevention through HHIT registration
  - Appendix A has collision formula

HHIT design compromises

- How many levels of hierarchy in 32 bits?
  - 14 bit Registered Assigning Authority (RAA)
    - 16,384
  - 18 bit Hierarchical HIT Domain Authority (HDA)
    - 262,144 per RAA
- How are top level numbers assigned?

HHIT design compromises

- How to distinguish flat from hierarchical HITs?
  - Choice between
    - Hierarchical HIT Suite IDs
    - Different Prefixes
- Recommend different Prefixes – reuse HIPv1
  - Limited number of Suite IDs
  - Only flat or hierarchy – 2 Prefixes
    - We need to get the hierarchy ‘right’ – DIRTFT

Impact on ORCHID construction

- RFC 7343 is designed for a 96 bit hash of HI
  - No flexibility
  - No support for hierarchy bits
- RFC 7343 cannot take advantage of new variable output hashes
  - SHAKE – NIST FIPS 202
  - cSHAKE – NIST SP800-185

Impact on ORCHID construction

- How should these changes to ORCHID be addressed?
  - Some are here
  - Some are in the new-crypto draft
- Should 7343 be directly updated?
  - i.e. all ORCHID changes in its own draft

Impact on ORCHID construction

- Python script soon available to create HHITs for testing.

Questions?