TM-RID BoF: Hackathon Report

IETF 106 – Singapore – Nov 19
Adam Wiethuechter
An overview of our time...

The #1 programmer excuse for legitimately slacking off:

"My code's compiling."

Hey! Get back to work!

Compiling!

Oh. Carry on.
OpenHIP build update

- Ubuntu 18.04 LTS builds for OpenHIP
  - Original stables were on Ubuntu 16.04, required manual work to get Ubuntu 18.04 build
  - Installs dependencies (apt and OpenSSL 1.0.1r)
    - OpenSSL 1.1.1 support coming in hipv2 branch (work being done by Gurtov students)
  - Makefiles updates to help to fix build
  - Will be branching off and creating PR soon on the Bitbucket
- Should make HIP development easier to start!
HHIT Generation Prototype

• Generates HHITs using EdDSA25519 key-pairs and offers some utilities in Python for signing and verifying

• Attempted update to use cSHAKE instead of SHA1
  - No direct cSHAKE implementation in Python to use
  - Used SHAKE128 instead (asking for length of 64 bits)
  - Need to more closely review and understand FIPS202 and 800-185
    • Probably need to actually just write a implementation of cSHAKE in Python...
UAS Demo Application

- Skeleton Java/Android implementation
  - One phone acting as surrogate UAS broadcasting over Bluetooth using HHIT as ID Type (as we are proposing)
  - Receiver phone app performs reverse lookup with HHIT, then a forward look to obtain TXT record and displays additional information received
- Setup BIND DNS servers with PTR and TXT records
  - TXT contains PII (as proof of concept), but eventually will be a HIP RR lookup to get HI for more exciting applications
- Similar demo has been done at UAS Test Site in NY
  - Working on prototyping Wrapper Authentication message with signature verification on receiver back home
- Huge shout out to James at AX Enterprize who answered some questions and helped remotely (even at close to midnight his time)
Overall Summary

• Super productive
  – Hooray stable current builds!

• Learned things
  – ACLs suck when you forget their existence…also they are not DHCPs friend when you want to demo something!
  – Makefiles are not that scary

• Semi-stressful, but fun
  – Thanks cSHAKE I guess
Next Steps

• Get cSHAKE for HHITs
  – Need Python implementation for script or just fold in OpenHIP itself

• Wrapper format prototype
  – Send side done (on real UAS), need work on receive side in app
  – HIP RR instead of TXT records

• More implementations for interoperability testing
Questions, Comments?