HIP 5201-bis Update

Robert Moskowitz
Verizon Telcom and Business
Tobias Heer
RWTH Aachen University

March 31, 2011

rgm@labs.htt-consult.com
heer@cs.rwth-aachen.de

Purpose of this presentation

- An update on HIP BEX, rfc5201-bis progress
  - Crypto Agility
  - General Changes
  - Editorial Changes
  - What's Left

Crypto Agility

- Crypto Agility for signature algorithms
- Crypto Agility for hash functions
- Real Crypto Agility for DH (not just “pick one from two”)
- This also includes:
  - HIT, RHASH, HMAC
- ECC and SHA-X for HIP

General Changes

- Rename some Parameters (e.g. HIP_MAC) to make them more general
- Better Security Considerations Section (it seems rather outdated)
- Introduced lists for negotiation
  - DH List, HIT Suite List
- Increase Version Number and change title of document

Editorial Changes

- Many clarifications
- Better Terminology section
- Clearer Parameter descriptions
- Fixed some remaining bugs and inconsistencies from 5201

What's Left

- Use List-based negotiation for transport formats (ESP)
  - Requires changes to the ESP document RFC5202-bis
- OGA in ORCHID document
  - Note prefix NOT listed by IANA
    - If so, BackToMyMAC MAY have used HIP instead of reinventing pieces of HIP
- IESG comments on 5201 datatracker.ietf.org/doc/draft-ietf-hip-base/writeup/
  - Randomize hashing in signatures (should be quick)
  - Negotiation of KDF
  - Combine encryption modes

What's Left

- More IESG comments on 5201
  - Different RSA mode OAEP/PSS
  - Crypto Agility for HMAC
  - SHA-1 is outdated (we covered that)
  - Use of incoming IP addresses
    - Might affect MM draft, too
  - Interactions with complex SPDs may result in weird effects

Questions?