Status of
draft-heer-hip-lhip-00.txt and
draft-heer-hip-midauth-00.txt

Tobias Heer

Distributed Systems Group
Chair of Computer Science IV
RWTH Aachen University
http://ds.cs.rwth-aachen.de
LHIP: Short Recap

- Light-weight HIP
  - Resource-constrained devices
  - Reduces PK cryptography
  - Hash chain based auth
- Useful also for middleboxes
  - Cheap authentication
- Two modes
  - Authenticated mode (with RSA/DSA)
  - Unauthenticated mode (no RSA/DSA)
    - Anonymous service
- Touches many aspects of HIP
LHIP: Feedback

- Slow BEX is not a major issue
- Load on middleboxes is an issue
LHIP: Status

- LHIP has been „on hold“ for a while
- Stronger focus on middleboxes
- Focus on authenticated mode
  - Full HIP BEX plus hash chains
  - LHIP only for speeding verification by middleboxes
  - Fewer changes to HIP
draft-heer-hip-midauth-00
HIP Authentication by Middleboxes

1.) Authentic Base EXchange:

2.) Replay:
Midauth: Short Recap

- Mitigate replay attack targeting middleboxes
- HI authentication by middleboxes without explicit registration
- Middleboxes participate in BEX and Update
  - Inject nonces into HIP control packets
  - Puzzles to protect middleboxes
Midauth: Feedback

- Letting RESPONDER solve puzzle is a bad idea
- PUZZLE_M / ECHO_REQUEST_M format
  - One vs. two distinct parameters
- Security implications for the payload channel?
Midauth: Status

- Address puzzle issue:
  - Only INITIATOR solves puzzles
- Condense PUZZLE_M and ECHO_REQUEST_M to one parameter
- Separate discussion of control and payload channel
- Add usecases
- Collaboration with Julien Laganier and Miika Komu