HIP Backgrounder

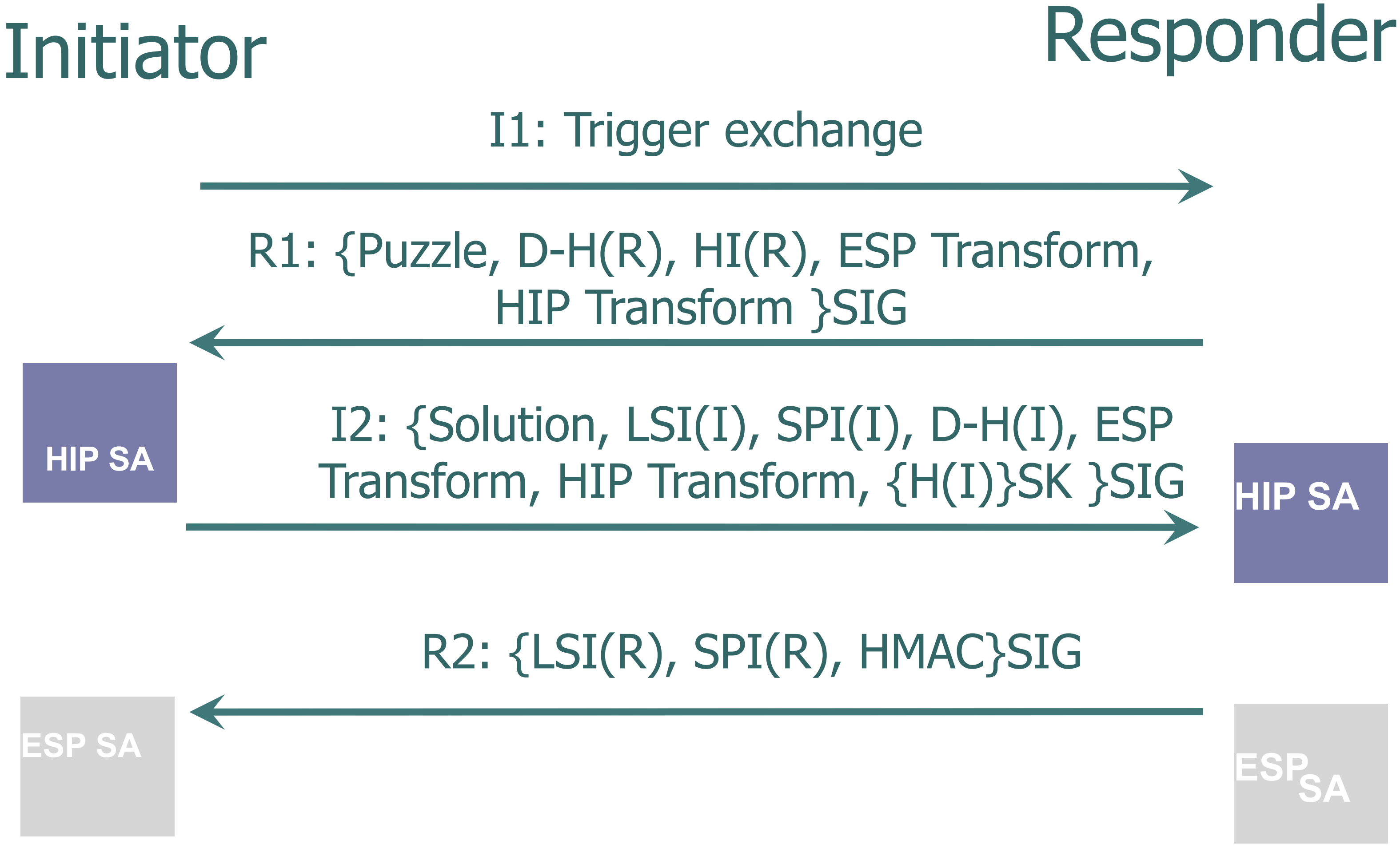
What REALLY is the
Host Identity Protocol

Robert Moskowitz
HTT Consulting
July 19, 2017
IETF 99, Prague CZ

The Host Identity Protocol

- Based on a ‘new’, ‘flat’ Namespace:
  - The Host Identity Tag
    - A valid, non-routable, IPv6 address
- HIT cryptographically derived from the Host Identity
  - ‘Raw’ public key: RSA, DSA, ECC
- Minimalist SIGMA compliant protocol to exchange Identity/Identifier plus other information between peers
  - SPI (4 byte Security Parameter Index) as per packet Identifier

HIP Base Exchange



Initiator

Responder

I1: Trigger exchange

R1: {Puzzle, D-H(R), HI(R), ESP Transform, HIP Transform }SIG

HIP SA

I2: {Solution, LSI(I), SPI(I), D-H(I), ESP Transform, HIP Transform, {H(I)}SK }SIG

HIP SA

R2: {LSI(R), SPI(R), HMAC}SIG

ESP SA

ESP SA

- Every packet contains HIT(I) and HIT(R) in the header.

HIP Mobility

- Concept of a Rendezvous Service
  - Peer registers to an RVS using HIP-REG
  - Peer publishes RVS as its LOC
  - Initiator sends I1 to RVS
  - RVS forwards I1 to Peer
  - Peer sends R1 directly to Initiator
- RVS ‘sling shots’ I1 to peer and has no further interaction until...

HIP Mobility 2

- A Peer moves…
  - Sends a HIP-NOTIFY with new LOC to
    - Peers
    - RVS
- When both Peers move at the same time
  - ‘Double Jump’
  - HIP-Notify to Peer ‘misses’, but can relearn from RVS
  - Accelerated with new fast-mobility draft
    - Uses ‘shotgun approach’

Using HIP

- Peer to Peer tunneling of HIT-based connections using SPI in actual tunnel
  - HIP enabled ESP in Bound End-to-End Transport (BEET)
  - Draft on Secure Session Envelope and Secure Session Layer Services
  - Draft on unsecured HIPnIP (variant of IPnIP)
- HIP should NOT be about simpler ESP, but connecting 2 Endpoints

Weakness in HIP

- Too much Crypto!
  - Shim6
  - HIP Diet Exchange (HIP DEX)
  - HIPnIP
- Change in IP stack behavior (HIT to Loc maps)
- HIT discovery
  - DNS RR for FQDN to HI/HIT
  - Reverse lookup (only DHT experiment)

New HIP work

- Hierarchical HITs
  - Adds domains and registration services
- Fast Mobility
  - Shotgunning and Piggybacking
- New, faster Crypto
  - Stay tuned for Edward curves and Keccak algorithms