Update

draft-hip-heer-midauth-02

(Tobias Heer, Miika Komu, Klaus Wehrle)

Changes Since Version 01

- Parameter structure
- Editorial changes

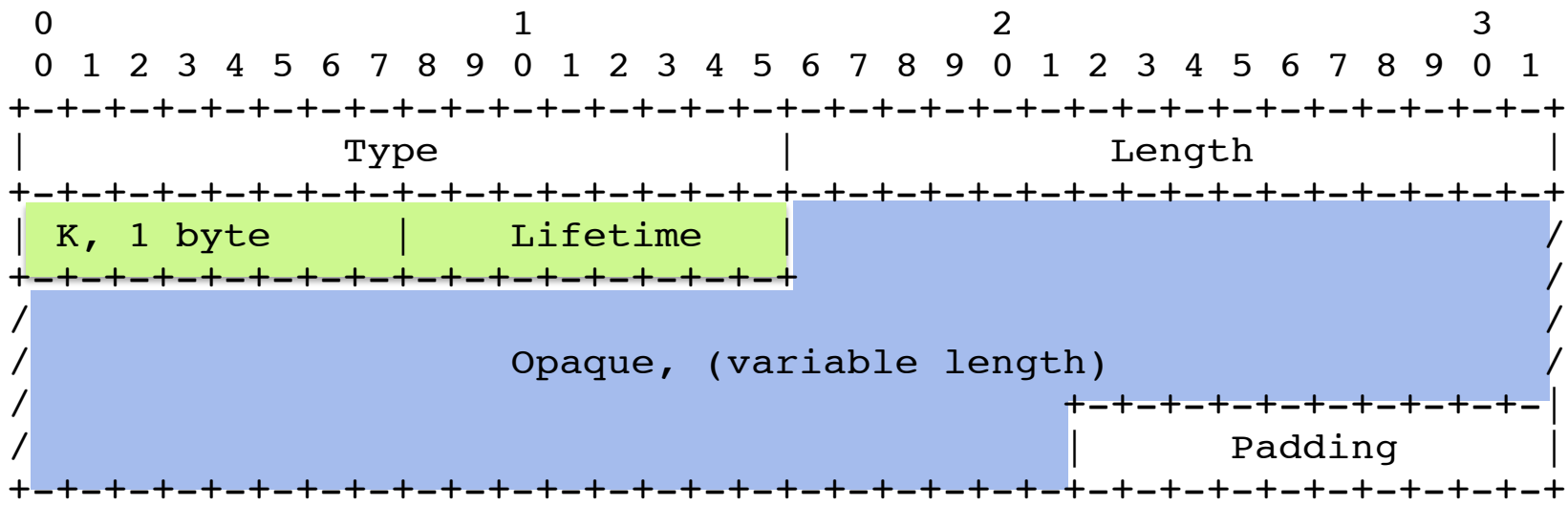
Merged Puzzle + Nonce

Reordering issue with two MBs:

Puzzle1, Nonce1, Puzzle2, Nonce2 → Puzzle1, Puzzle2, Nonce1, Nonce2

ECHO_REQUEST_M PUZZLE_M

CHALLENGE_REQUEST

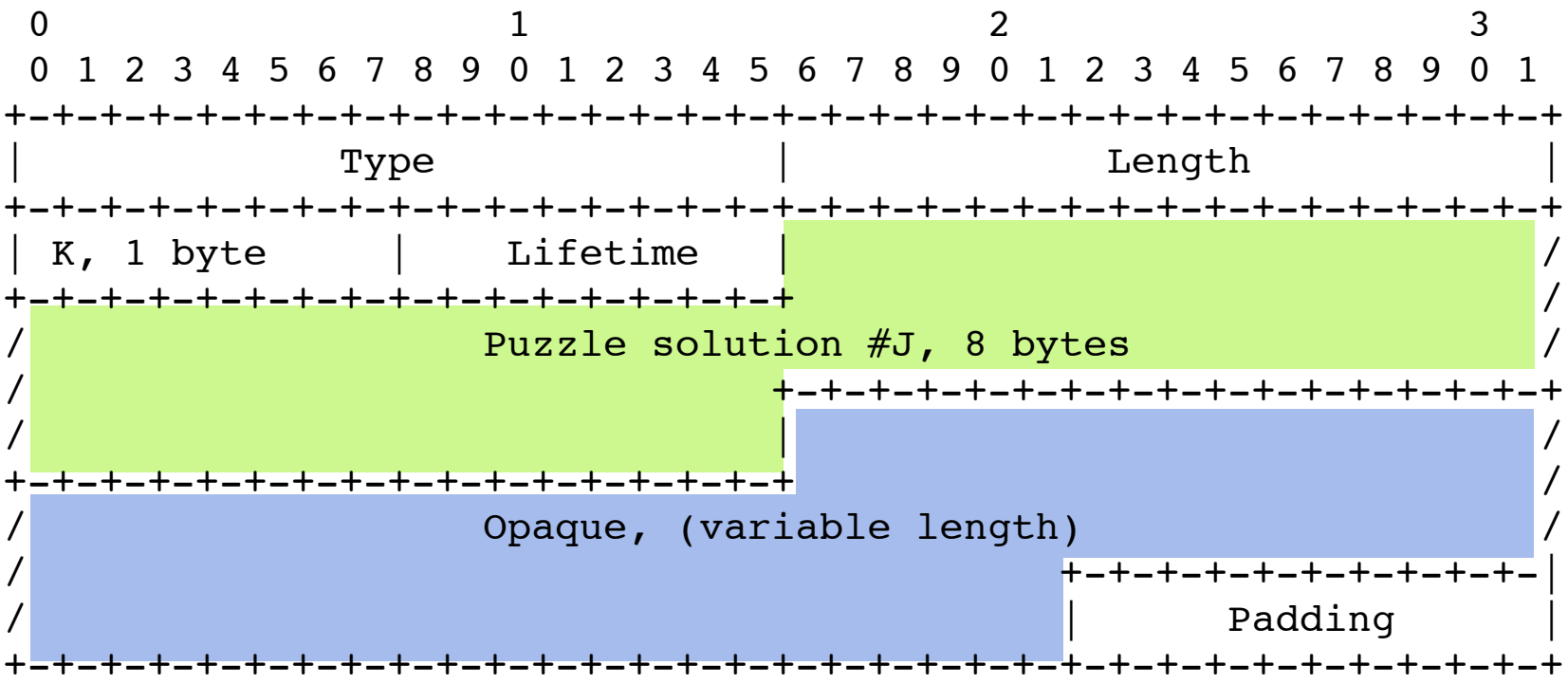


Where is the Puzzle Seed?

- Apply hash function to OPAQUE field to generate puzzle seed
- Saves some bytes for seed in CHALLENGE_REQUEST
- Opaque field should exhibit sufficient randomness
- Middlebox can add randomness to OPAQUE field if needed

Merged Solution and Response

CHALLENGE_RESPONSE



New Draft

Service Identifiers for HIP

draft-heer-hip-service-00

(Tobias Heer, Samu Varjonen, Hanno Wirtz)

Services for HIP

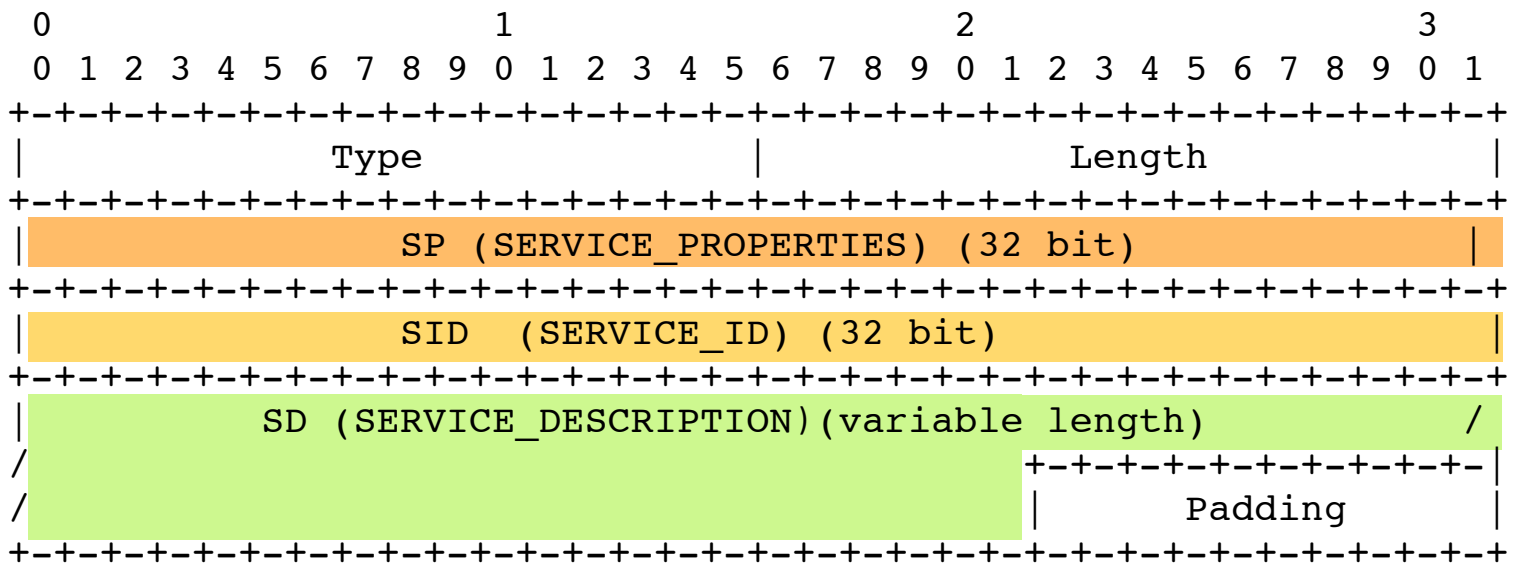
- Services: static, dynamic
- Description: static, dynamic
- Offered services can even depend on requester
- Offered by end-hosts and middleboxes
- Some services require additional credentials (certs, ACL)

REG_INFO

- Quite simple (just a number)
- Always in signed part of the packet

SERVICE_OFFER

- Service properties: classification (understood by everyone)
- Service ID: identifier for a service
- Service description: service-specific details
- 2 flavors – signed and unsigned



SERVICE_OFFER (cont‘d)

- Transmitted in R1, I2, R2, UPDATE
- **Signed:** for end-hosts
- **Unsigned:** for end hosts and middleboxes
  - End hosts? → R1 pre-creation and dynamic services
  - Middleboxes: adding offers to HIP packets

SERVICE_ACK

- Acknowledges a subset of the set of offered services
- Echoes hashed service offer as service contract
- In signed part of the packet (contract)

Service Properties

- Bit-field with general information about a service
- Classification
- Anyone interested in helping to define the properties?
- Send e-mail to: heer@cs.rwth-aachen.de

Service Properties Field

- 0 REQ - Required
- 1 COM - Commercial
- 2 FOR - Forwarding
- 3 TER - Terminal
- 4 INI - Initial
- 5 ACI - ACL Initiator
- 6 ACR - ACL Responder
- 7 CEI - Cert Initiator
- 8 CER - Cert Responder

More suggestions and requirements?