SHIM6 Privacy Analysis
draft-bagnulo-shim6-privacy-00

Marcelo Bagnulo
shim6 wg
IETF 65 - Dallas
ULID-pair Context Establishment Exchange (I)

• Sensitive Information in I1 packet
  – ULID-pair option (related to locator pair)
  – Context tag

• Sensitive Information in R1 packet
  – none
ULID-pair Context Establishment Exchange (II)

• Sensitive Information in I2 packet
  – ULID-pair option
  – Context Tag
  – Locator Set option
  – CGA Parameter Data Structure Option
ULID-pair Context Establishment Exchange (III)

- Sensitive Information in R2 packet
  - Context Tag
  - Locator Set option
  - CGA Parameter Data Structure Option
Packets with the Payload header

- Possibility of correlating packets with different locator pairs using the context tag
- Bind different locators to a single host
Update messages

• Sensitive Information Update Request
  – Context tag
  – Locator pair list
  – CGA Parameter Data Structure

• Sensitive Information in Ack
  – The context tag
  – Nonce information (if different locators are used)
Keepalive & probe messages

- Context tags
- Identifier
Solution space

• For most of the information in I2, R2, Update, Probe, Keepalive:
  – Negotiate shared secret (DH) and encrypt

• For context tags
  – Need that different locator pair carry different CT. CT must be known beforehand by the peer.

• For I1 message:
  – Remove sensible information or,
  – Add previous message exchange to negotiate a shared secret
Do we (need to) care about this?