multi6 design team #1

status update

IETF 58 Minneapolis 2003

Tony Li (chair), Erik Nordmark, Sean Doran, Pekka Savola, Mike O'Dell, Dave Katz, Brian Carpenter, Steve Bellovin, Iljitsch van Beijnum

loc/id separation

- Identifiers are stable, for use by transport protocols and applications
- Locators are subject to change, used to navigate packets through the network
- Traditionally the IP address has always served both functions
- DT has adopted shim layer between IP and transport as working

DT considering

- Drafts:
  - Threats
  - NOID
  - SIM-CB128
  - CB64
- Missed cutoff:
  - cryptoid.txt

Threats draft

- Erik Nordmark will be presenting
- Allowing locator change = security holes
- Means additional work required (reverse lookups, crypto) to plug these holes
- Similar to Mobility in IPv6 (thanks guys)
- However, can't just use MIPv6 mechanisms (Erik will tell you why!)

NOID

- There is no identifier beyond the FQDN
- (But we're not making the FQDN do additional ID work either)
- ULP uses a single locator during (its idea of) a session
- Shim layer recovers additional locators through reverse⇒forward⇒reverse DNS
- Then changes locators when needed

SIM-CB128

- Secure Identity Multihoming 128 bit crypto-based identifier
- Identifier is 128 bit hash of a public key
- ID is similar to HIP, rest is different
- FQDN points to both ID and locators
- Can't map from ID to locators or FQDN
- Rehoming secured by PK crypto exchange
- No PKI: key is authenticated by hash in ID

CB64

- Similar to SIM-CB128, but shorter hash
- Allows for both locator and ID part in IPv6 address which can be in reverse DNS
- Also similar to NOID as ULPs see locator bits (but those no changes during session!)
- ULP and application aren't aware of ID vs locator bits

"cryptoid.txt"

- No acronym yet, missed cutoff (2 x ouch)
- Very similar to CB64
- But identifier has internal structure:
  - 44 or 48 bits site ID (= hash)
  - 12 or 16 bits host ID (= just a number)
- Expand/contract 64 ⇔ 128 bits
- Allows hiding locator from ULP but have both locator and ID bits on the wire

Stay tuned

- Tomorrow at 9:00 Erik will be talking about:
    - Threats
    - NOID
    - SIM CB128
    - CB64