Applying CGA and CBA to Mobile IPv6

Revision of draft-arkko-mipshop-cga-cba-04.txt

Jari Arkko ⟨jari.arkko@ericsson.com ⟩
Christian Vogt ⟨chvogt@tm.uka.de⟩
Wassim Haddad ⟨wassim.haddad@ericsson.com ⟩

Look Back to Previous Draft Version

- 2 independent optimizations
  - CGA-based home address ownership proof supersedes periodic home address reachability test
  - CBA permits secure, concurrent care-of address test
- Previous draft version (03) says:
  - “The protocol consists of two individually applicable optimizations for the home and care-of address tests. […] For convenience, this overview shows both optimizations applied together.”
- But: Protocol description glued optimizations together

Optimizations Now Orthogonal

- Revised protocol description
  - Optimizations now individually applicable
    - Home CGA + CBA (preferred, since most efficient/secure)
    - Home CGA + standard care-of address tests
    - Standard home address test + CBA
- Clearer draft structure
  - Objectives
  - Protocol design
  - Protocol operation
  - Option Formats and Status Codes

Optimizations Now Orthogonal

- Permanent home keygen token replaces permanent shared key KBM_{perm}
  - Token obtained in the same way as shared key
    - During initial handshake
    - Encrypted with mobile node's public CGA key
    - Valid for 24h
  - Calculate KBM + authenticator as in RFC 3775
    - w/permanent home keygen token if home CGA
    - w/temporary home keygen token if regular home address

Optimizations Now Orthogonal

- Home keygen token retrieval
  - Home CGA ⇒ initial handshake ⇒ permanent home keygen token
  - Regular home address ⇒ home address test for each handoff + periodically ⇒ temporary home keygen token
- Care-of keygen token retrieval
  - Using CBA ⇒ early Binding Update first, then care-of address test, then full Binding Update
  - Not using CBA ⇒ care-of address test first, then full Binding Update

Question for Working Group

- Allow for CGA-based address ownership proof for correspondent node?

Institute of Telematics
Universität Karlsruhe (TH)
www.tm.uka.de