draft-ietf-mipshop-cga-cba Status Update

Jari Arkko, Christian Vogt, Wassim Haddad

IETF 67, Mipshop Session, San Diego, Nov. 7, 2006

Acknowledgment

- Several excellent reviews. Thanks!
  - James Kempf
  - Vidya Narayanan
  - Lakshminath Dondeti
  - Zhen Cao
- Previous contributors
  - Pekka Nikander, Tuomas Aura, Greg O'Shea, Mike Roe, Gabriel Montenegro, Vesa Torvinen, Greg Daley, Samita Chakrabarti, Marcelo Bagnulo, Suresh Krishnan, Mohan Parthasarathy, Lila Madour, Francis Dupont, Vijay Devarapalli, Roland Bless, Mark Doll, and Tobias Kuefner

Discussion Before WGLC

- Does HoA ownership proof redundantize CoA test for reachability verification?
  - RFC 3775: Trust between MN and HA
    ⇒ No CoA test necessary for home registrations
  - RFC 3775 is not very clear where this trust is based upon
    (1) On administrative relationship between MN and HA?
    (2) Or on strong IPsec security relationship between MN and HA?
  - Option (1) is true
    - Same rationale in RFC 4449, "Securing Mobile IPv6 Route Optimization Using a Static Shared Key"
  - Option (2) is incorrect
    - CNs are unaware of HoA ownership proof
      ⇒ Strength of HoA ownership proof does not matter
    - Assuming option (2) is right leads to following **false** conclusion:
      - Strong CGA-based HoA ownership proof in correspondent registration
        ⇒ No CoA test in correspondent registration needed
  - Therefore, CoA test required despite CGA-based HoA ownership

Discussion Before WGLC (cntd.)

- Revised security considerations address this and other topics, including…
  - Why we need initial HoA reachability verification despite the CGA-based HoA ownership proof
  - Why we bootstrap a shared key from the initial CGA-based HoA ownership proof
  - Why we don't need CGA-based CoAs

Comments During WGLC

- Document technically correct, but adding diagrams would make it more understandable
  - Will do that.

- Document currently specifies 384-bit minimum length for RSA keys. Need higher minimum?
  - Requires more discussion…

Minimum RSA Keys Length

- Why minimum RSA key length matters:
  - Security of CGA normally determined by length of hash extension
    - Difficulty is finding right modifier
    - Length of hash extension encoded into CGA (3-bit Sec value)
      ⇒ Downgrading impossible
  - However: Difficulty of finding right modifier is zero if attacker integer-factors RSA public key
    - Attacker can then simply copy CGA owner's modifier
- Higher minimum RSA key length mitigates this threat
  - Requires secure binding CGA ↔ minimum key length
    to prevent downgrading

Minimum RSA Keys Length (cntd.)

- Possible solutions:
  (1) "Hard-code" longer RSA keys into protocol specification
    - Easy, but no crypto agility

  (2) CN defines minimum key length + Error code for Binding Acknowledgments indicating that MN's keys are below minimum
    - A bit more complex, but crypto agile

  (3) MN defines minimum key length, encodes it into CGA
    - Easy and crypto agile
    - Requires minor changes to draft-bagnulo-multiple-hash-cga
- Not a solution:
  - MN sets minimum key length w/o encoding it into CGA
    - Attacker plays role of MN and could therefore choose minimum key length ⇒ Downgrading possible
- Which solution? Which key length? Recommendations?