Registration Revocation in Mobile IP

Comments, Issues, and Solutions
from WG, and IETF Last Call
(the big ones, at least)
draft -05 --> -06

Steve Glass – Sun Microsystems
Madhavi Chandra – Cisco Systems

Replay Mechanism Don't We Already Have One?

- Why not use RRQ/RRP IDs?
  - These protect the MN and HA from replay, **NOT** FA!
  - Doesn't scale for 'batch' revocations ('M' bit)
    - 'Borrowing' RRQ/RRP IDs may even be LESS secure?
    - What happens if the 'exemplary' binding expires?
    - ...
  - RRQ/RRP IDs could be NONCES!
    - Call me 'legally paranoid'
    - I'm not a lawyer, nor do I want to play opposite one on TV
    - Gives us an excuse for something better (IM[NS]HO)

Replay Mechanism: We Do Have Time Stamps

- Use [of] Time Stamps
  - Scales better in general (also less to remember!)
  - Used with peer-SA.
  - Faster Processing.
    - No need to e.g. run through all previous values.
    - Time Stamps ~ nonces 'with a pattern'.
  - Requires a time stamp in the revocation extension.
    - Gives a 'start' time to each and every [re]registration.

About Time Stamps

- They're not Global! They're per-agent [per-SA],
  - (per-binding if you prefer, but you can simplify this).
  - Used in combination with Home Address field.
  - Seconds (4 bytes) or seconds+fractional (8 bytes)?
  - Whichever meant adding to Revocation Extension (RRQ + RRP) + Revocation Message.
  - Combined w/ 3344's 1 registration/second, seemed logical to only allow 1 revocation/second (we're talking per binding [set], of course).
  - > Seconds easily justified, fractional seconds less-so.

Revocation Scope

- Recall: Revocations are “FYI”
  - Must be. Can't force an agent to keep a binding!
- Scope MUST only be bindings shared w/ peer.
  - Seems obvious, but...
- If 'M' bit is supported, then:
  - Have access to IPsrc, or
  - Have a way to determine scope via SA [NAI]
- Else, 'good' agent can imply wrong scope!

Security Issues

- Use Challenge/Response
  - RRQ/RRP can BOTH be replayed (from 3344)
  - Leads to revocation replay! Bad if 'M' bit was used!!!
- 'M' bit considerations”
  - More 'up for grabs', use stronger security (e.g. IPsec)!
  - Know where the Revocation came from!
    - Consider good HA x.y.z.t, revoking MNs in a.b.c.0/24
  - MUST understand prefix-length outside the scope of agent advertisements (type 19 = throw it all away)

Other “Past-Over” Issues

- 'Direction' bit
  - HA sets a bit, helps against reflection attacks
  - But, agent can be HA to one MN, and FA to another
  - Overlapping private addrs -> both have same Ipaddr
  - > Edge: MUST use IPaddr, and Time Stamp anyway
- Error codes
  - If there's a problem, could be good to relay it.
  - But, revocation isn't 'negotiated', it's FYI.
  - FWIW, I have yet to see a useful error.

Late Comments, but...

- Advertisement 'X' bit position corrected!
  - Conflicted with NAT Traversal draft!
- Added 'IANA Consideraions'
  - 2 New Message Types,
  - 1 New Extension,
  - 1 New Use of a pre-existing extension.
- Thanks to those who gave comments (even late)!
  - Yes, I had no time, but still want it to be right!