Generic Notification Message for Mobile IPv4

- Issues from WGLC

(draft-ietf-mip4-generic-notification-message-06.txt)

Post LC Comments

- Discussion threads:

http://www.ietf.org/mail-archive/web/mip4/current/msg03088.html

http://www.ietf.org/mail-archive/web/mip4/current/msg03104.html

Key points of discussion

-“MN-FA and FA-MN, this scenario is NOT addressed in RFC3344 and THUS it is new with new security architecture and requirement that you MUST clearly identify and address. Although, it may sound as if RFC3344 is addressing this case but it is NOT.”

-“A security architecture that address all applicable security threats for this end-to-end signaling, for example saying that the Identification field is used for replay protection does not mean anything. You need to clearly articulate how replay protection mechanism is used in each case. How you security architecture address Man-in-the-middle attack, etc.”

Key Points of Discussion (Contd.)

- “A security architecture that address all applicable security threats for an end-to-end signaling between the FA and the HA. For example, in RFC3344 the HA is always receiving RRQ but sending RRP, different messages, do you see the difference. Instead of you looking into RFC3344, you SHOULD look into RFC3543, Registration Revocation in Mobile IPv4, Security architecture. It is more relevant.”
- “You MUST remember that the FA and the HA MAY belong to different operators and there has to be some assumption of how these two nodes establish their security association. Please remember, All operators that I am aware of HATE statically configured shared secret keys. Please keep that in mind. Although, statically configured shared key MAY just a distant MAY be possible between the MN and its HA, but unlikely between the FA and the HA across different domains.”
- Revisit the message format and identify the parameters that may not be needed. Ex: HA Address in the Notification Ack.

Response to the Comments

- The semantics provided by 3344 with respect securing signaling messages in all the three paths (HA-FA, FA-MN, HA-MN) are sufficient for securing Generic Notification messages. However for replay protection additional considerations may be required.
- The draft requires an established security association between the mobility agents for exchanging the notification messages. It includes provisioned keys, authentication algorithms and other relevant parameters. It is out-of-scope for the Notification draft to define a new security architecture, message protection mechanisms, or SA establishment protocols.
- The draft has no relation to RFC-3543.

Next Steps

- Numerous editorial issues that have been identified from Kent's and Ahmad's review have to be discussed and resolved.

  - Review the message fields and fix the message parameters.

  - Address re-sync issue. RRQ/RRP MUST be used for re-sync. Specify considerations for foreign-agent with respect to handling error code 133 (Id Mismatch) with respect to time synchronization.

  - Add text for clarity with respect to securing messages.

- Specify new examples for the Notification message use-cases.

- Will revise the document based on this input.

Thank You