IETF-55

Mobile IP WG
RFC3012bis Issues

draft-ietf-mobileip-rfc3012bis-03.txt

charliep@iprg.nokia.com
pcalhoun@diameter.org
jayshree@nortelnetworks.com

Lost Registration Reply

Issues:

- What happens when Registration Reply is lost?
- Why not have the "keep N+1 challenge values" apply to the values sent in both advertisements and replies.

Description:

- When Registration Reply is lost, the Mobile Node will perform retransmission (as per RFC3344) with the same challenge value.
- The FA treats the retransmitted request as new Request and generates PREVIOUSLY_USED_CHALLENGE (terminology TBD) error code.
- Do we need explicit description on Registration Reply processing in the draft?

Use of Challenge Between FA and HA

Issue:

- Non ideal usage of Mobile-Foreign Challenge extension between the FA and the HA

Description:

- Currently no explicit mechanism for the protection against the bogus Registration Reply if there is no SA between the FA and the HA.
- If removed, causes backward compatibility with RFC3012.

FA Invalidating Auth Data of HA

Issue:

- The FA invalidates the authentication data supplied by the HA in the Mobile-Home Authentication extension to the Registration Reply. Thus, a malicious node might try to supply a bogus Registration Reply to the MN

Description:

- The challenge extension is added after Mobile-Home Authentication extension.
- Remove the second paragraph from section 12?

Terminology

Issue:

- Current definitions of “Previously Used Challenge” and “Stale Challenge” are confusing (section 1.1)

Description:

- Suggestion is to combine both definitions with one the following terminology
  - Previously used challenge
  - Stale Challenge
  - Expired
  - Duplicate
- Any suggestion on terminology (and name of error code to reflect this terminology) ?

Backward Compatibility

Issues:

- The FA is required to reject the reply if challenge is not included
- The FA implementing RFC3012bis is not allowed to interoperate with a HA which does not implement functionality provided by RFC3012bis

Description:

- The HA doesn't add the challenge extension if it is not supported (section 3.4)
- The FA should include a new challenge extension in any Registration Reply, successful or not (section 3.3)

New SPI for HMAC-MD5

Issue:

- MD5 is less secure than HMAC-MD5 (SPI for Radius server)

Description:

- RFC3012bis draft is updated to optionally support additional SPI called HMAC_CHAP_SPI
- If HMAC_CHAP_SPI is received in a Generalized Mobile IP Authentication extension, the HMAC-MD5 will be used instead of MD5 for computing the authenticator (section 8)

Challenge in Bogus Registration Reply

Issues:

- Protocol subject to bogus Registration reply
- Since every Registration Reply includes challenge, the bogus Registration Reply must be accepted by the MN

Description:

- The challenge received in the bogus Registration will be rejected when it is applied for the new registration by the legitimate Foreign Agent.