draft-ietf-dime-e2e-sec-req-01

DIME WG – IETF88

Hannes Tschofenig
Jouni Korhonen
Glen Zorn
K. Pillay

Background

- It is a well-known fact that Diameter base protocol has no end-to-end security.
  - To be fixed with a new attempt.. and now more topical than ever ;-)
- From the current charter:
  - Dec 2012 - Submit 'problem statement and requirements for Diameter end-to-end security framework' to the IESG for consideration as an Informational RFC
  - Well.. are almost there ;-)

Current status

- Authors think the document is “almost there”
- Two open issues (also written down in the I-D)

Open issue #1 - Capability/Policy Discovery

- This document talks about selectively protecting Diameter AVPs between different Diameter nodes. A Diameter node has to be configured such that it applies security protection to a certain number of AVPs.
- A number of policy related questions arise:
  - What keying material should be used so that the intended recipient is also able to verify it?
  - What AVPs shall be protected so that the result is not rejected by the recipient? In case of confidentiality protection the Diameter node encrypting AVPs needs to know ahead of time what other node is intended to decrypt them. Should the list of integrity protected AVPs be indicated in the protected payload itself (or is it known based on out-of-band information)?
  - Is this policy/capability information assumed to be established out-of-band (manually) or is there a protocol mechanism to distribute this information?

Open issue #2 - Command-Line Support

- Should solutions allow the provisioning of long-term shared symmetric credentials via a command-line interface / text file? This allows easier management for small-scale deployments.

Next steps

- Fix the issues.
- WGLC.. Ok?

Questions ?

Jouni will pay attention just like in v6ops session…