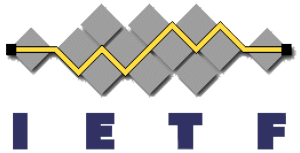
Transport Layer Security-based Mobile IPv6 Security Framework for MN Node to HA Communication

IETF#80 MEXT WG, 1-April-2011

draft-ietf-mext-mip6-tls-00

J. Korhonen, B. Patil,

H. Tschofenig, D. Kroeselberg



General

- Background:
  - A DSMIPv6 solution using TLS as the security protocol instead of ESP, and a specific “HAC function” for bootstrapping the MN and provision the HA.
  - First individual submission July 6, 2009.
  - MN & HA implementations around for Linux (including N900..)

- Approved to WG (as per current charter) with an experimental track status.

On going discussion

- We got few extensive reviews (thanks to Domagoj, Ruyji, ..) that pointed out several places to clarify & enhance.

- Lack of route optimization:
  - Lets add it (originally route optimization was scoped out from the I-D..)

- Encapsulation discussion:
  - Currently the I-D defines UDP encapsulation with TLS encryption and a very similar encapsulation to ESP. Thus, why not using ESP then?! Because the original proposal _was_ to avoid IKE/ IPsec all together.. the packet formats just look ~about the same.
  - The discussion saturated on the list but continued offline with smaller group of people.

Next steps..

- Address the obvious review comments.. nits and alike..
- Start with the route optimization:
  - Would that mean old style return routability test, or
  - could that mean placing a HAC to a CN, and skip return routebility test (the HA would not be needed then at all for route optimization)
- Figure out whether current TLS-based encapsulation needs to be changed to something else..
  - The authors encourage people to bring concrete proposals to the mailing list & authors and then find a consensus among those.