AAA-based Handover Keys

MIPSHOP WG, IETF 70

Vijay Devarapalli (vijay.devarapalli@azairenet.com)

Current status

- We have a charter item on standardizing a mechanism based on the AAA infrastructure to generate handover keys for FMIPv6
- There is WG consensus to work on this
  - Was re-confirmed at the last IETF meeting
    - The do-nothing option was rejected
- Multiple solutions available
  - Three options on the table

Option #1

- Handover key management protocol between the mobile node and the access router
  - Mobility Header used for the messages
  - Assumes a shared key between the MN and a handover server (presumably AAA)
  - http://tools.ietf.org/html/draft-vidya-mipshop-handover-keys-aaa-04
- There was consensus early 2006 to adopt this document
  - But there was a delay in getting security reviews
  - Few other process related issues
- Not sure if there is WG consensus still on this document
- Authors have lost interest in this draft

Option #2

- Based on deriving a FMIPv6-specific key from a shared key between the MN and the NAS
  - The shared key is assumed to be the EAP MSK
- draft-yegin-fmip-sa-00.txt
  - http://tools.ietf.org/id/draft-yegin-fmip-sa-00.txt
- Applicable only when EAP is used for access authentication

Option #3

- HOKEY- based solution
- Write a document in MIPSHOP WG that describes how to generate FMIPv6-specific handover keys from the USRK
- Only applicable when EAP is used for access authentication
- Would need message exchanges between the MN, the AR and the AAA to generate a FMIPv6 handover key from the USRK
  - If USRK is delivered to the AR, then the message exchange can be restricted to the MN and the AR

Next Steps

- Pick one solution to standardize
  - Add the specific solution to be standardized to the charter
  - Status may be Experimental or Proposed Standard
- Would like to hear from people…