AAA-based Handover Keys

MIPSHOP WG, IETF 72

Vijay Devarapalli (vijay@wichorus.com)
Stefano Faccin (smfaccin@marvel.com)

Current status

- FMIPv6 requires a shared key between the PAR and the mobile node for securing FBU/FBAck signaling
- A SeND based solution for setting up a security association between the mobile node and the access router has already been standardized
- We have a charter item to work on a AAA-based solution for setting up the security association

SeND-based FMIPv6 Security

- Requires the deployment of SeND in the access network
- May not be a feasible solution for many access networks

AAA-based Handover Key solutions

- There are three proposals
- Derive a MN-AR key from a HOKEY USRK
- Develop a Key Management Protocol as described in draft-vidya-mipshop-handover-keys-aaa
  - Assumes a shared key between the MN and the handover key server (presumably AAA server)
- Derive a FMIPv6-specific key assuming a shared key between the between the MN and the NAS
  - Described in draft-yegin-fmip-sa

FMIPv6 Security

- It looks unlikely that any of these solutions get used with FMIPv6
- Expect the SDOs to use access specific mechanisms to secure MN-AR signaling
- Too little information to pick one of the solutions for Proposed Standard status

Next Steps for AAA-based Handover keys

- Write an Informational document that says the AAA infrastructure can be used for setting up MN-AR security associations
- Gives the impression that SeND is not the only solution
- Will refer to the existing solution documents for possible solutions
  - The existing solution documents will not be standardized
- We can develop a solution later
  - If there is a sufficient interest in a particular solution
  - Or if a AAA-based security solution actually gets deployed with FMIPv6