Issues beyond the base RFC

- Parallel RFCs and future RFCs

MIPv6 Design Team

March 19th, 2002

Parallel and/or future RFC work

In order to produce a base MIPv6 RFC soon…

… work should be done in a separate RFC if it is

- not absolutely essential for MIPv6 to work,
- has some issues that need to be specified and analysed, AND
- is technically possible to add later in a backward compatible way

Parallel and/or future RFC work

1. Capturing the design decisions behind MIPv6
2. Piggybacked signalling on payload packets
3. Binding Security Associations for improved RR performance
4. Use of unverified Home Address Options
5. Stronger IFL authorization mechanisms, e.g. CGA
6. AAA-based IFB authorization mechanisms
7. Using IPsec as the sole MN-CN BU authorization mechanism

Challenge

- Which one is first submitted to the RFC editor:
  - The MIPv6 base specification
  - An extension to the MIPv6 base specification

Piggybacking

- Proposals exist, discussion on IPsec details and APIs, on whether to use another new header or DO
- Flag fields in the HOTI, HOT messages can be used to indicate support and desire for piggybacking
- After both peers agree to piggybacking, it can be used for all subsequent signalling
  - With the potential exception of 2a/2b that need IPsec protection from the HA to the MN

Unverified Home Address Option

- Proposals exist, discussion on socket API modification requirements etc.
- A node that supports unverified Home Address Option use can later optimistically assume the peer supports them too, and act on a Binding Missing message if it does not

Binding Security Associations

- Proposals exist, some security analysis remains
- Flag fields in the RR messaging can tell the peers if the other one supports a longer-lasting BSA
- For instance, if a HOTI/HOT can be omitted in quick movements, the COTI/COT messages can be run instead

Stronger IFL authorization

- Proposals exist, discussion on details, IPR, links to ND protection, …
- Bit method allows secure agreement whether to use RR or one of the better schemes (bidding-down)
- A selection between the better schemes can take place using flags in HOTI/HOT (bidding aside)

AAA-based IFB authorization

- No proposals
- Selection as for stronger IFL methods, or guided by AAA

IPsec as sole CN/MN authorization method

- Technically easy now with the new protocol
- Some security issues to describe when this can be allowed, what the certificates must contain etc
- Either flags or IPsec policy or both can be used to allow this.
- No bidding down problem if policy explicitly disallows RR and only allows IPsec-based MH
- RR can be turned off (if that's what we want) if MIPv6 and IPsec can talk to each other through an API