Currently Open Issues in the MIPv6 Base RFC

MIPv6 security design team

Editorial Issues

1. Many textual and editorial improvements needed
   - Please read the draft and comment
   - “parameter” -> “option”
2. Maximum binding lifetimes have to be specified in the document.
   - 5 minutes?
3. State tables or better behaviour descriptions to the CN, MN chapters?
4. Better terminoloy for ‘RR procedure’ ‘binding update procedure’
   - “RR procedure” is CoT/CoTI/HoT/HoTI?
   - “BU procedure” is RR prodedure plus BU and optional BA?
5. Better names for message types?

Open Issues

1. Bit method to prevent bidding down attacks?
2. How/whether to authenticate BA and BR?
3. Whether to authenticate the BM?
4. Should HAO be used in the Home Registrations or not?
5. How to secure home registrations, use ESP or AH?
6. Formatting issues: MH, fixed fields, parameters, ...
7. Is an SPI field useful?
8. Retransmission and nonce lifetimes
9. Do we need suboptions on HAO any more?
10. Does alternative CoA work with RR?

Bit method to prevent bidding down attacks?

- Discussion in IPv6 about *reserving* bits in interface IDs in progress
- *Using* reserved space requires a separate proposal in Ipv6 WG
- Proposed justification:
  - Mechanical semantics is “don't do RR”
  - Later bit might be redefined to mean e.g. That the IID is a hash of something – random number or public key [IPR likely here]

Bit method – next steps

- IPv6 WG will discuss reserving on Thursday
- Need to make proposal on usage for MIPv6

How and whether to authenticate the BA and BR?

- Need to be able to verify that they were sent in response to the BU?
  - An on-path attacker could of course spoof this
- Without check off-path attacker could spoof BA or BRs
- Adding a nonce in BU (returned in BA/BR) will do the trick?
- Similar issue for HoT/CoT
  - Include nonces in HoTI/CoTI as well?

Whether to authenticate the BM?

- When MN receives BM it checks in CN in Binding Update List
  - If no then must ignore BM
- Otherwise, unless too recent BM from CN,
  - Start RR procedure, or
  - Reverse tunnel
- The BM could still be spoofed by off-path attackers
  - Would cause some extra work but no ill effects

Should HAO be used in the Home Registrations or not?

- HA finds SA based on IPsec SPI + destination address
- Verifies src address against SA/SPD entry
  - Either the SA/SPD has a wildcard source, or
  - The HOA is used in the home BU
- Need to understand the tradeoffs here and pick

How to secure home registrations, use ESP or AH?

- ESP is needed for tunneled HoT; easier to do ESP for the home registrations?
- If ESP and HAO then the HoA/CoA will be included twice in the packet
  - In the IP src and HAO – not protected by IPsec
  - In the BU – protected by IPsec
- If AH and HAO is used then HoA just once

Formatting issues: MH, fixed fields, parameters, ...

- BUs to CN need authenticator and two cookies
- BUs to HA don't need this – just a sequence number to prevent reordered BUs
- Current plan is to define an authenticator parameter and a two-cookie parameter

Is an SPI field useful?

- A few algorithms can be identified using the flags field
  - Smaller packets
- Isn't needed for RR
- Probably not needed for RR with BSAs
- Can be added as a parameter by future schemes that need an SPI

Retransmission and nonce lifetimes

- When CoT, HoT, or BA is not received the MN needs to retransmit
- If the cookies in the BU are too old the CN will reject it
- How does MN know for how long it can use cookies?
- Should we just pick a constant? (e.g. 30 seconds)

Do we need suboptions on HAO any more?

- Originally all the DOs used *suboptions*
- Now everything but HAO is a separate message with *parameters*
- *Thus suboptions are only used for HAO*
- *Seems to make sense to drop the HAO suboptions?*
  - *Is there future undocumented usage?*

Does alternative CoA work with RR?

- Help us understand alt-CoA usage
- Implications of bombing attacks
  - CoTI sent with alt-CoA as source
  - COT sent back to alt-CoA with cookie computed for alt-CoA
  - BU can then be sent with *any source* and alt-CoA parameter
- Is this ok?

Deleting binding and replayed BUs?

- No state after BCE deleted
  - If BCE deleted (expired, or BU with lifetime zero) and nonce used to create it is still valid the BU can be replayed to recreate the BCE
- Need to retain information about BCE until nonce used to create it is invalid
  - Or make the nonce invalid once BCE deleted

Make BA mandatory?

- Needed for home registrations always
- Due to HAO verification it makes lots of sense to use BA for other BUs as well
  - Avoid data packets being dropped due to HAO if the BU is dropped in the network
- Suggestion:
  - BA not mandatory
  - Document the benefit of using BA
  - This allows unvHAO to be added separately