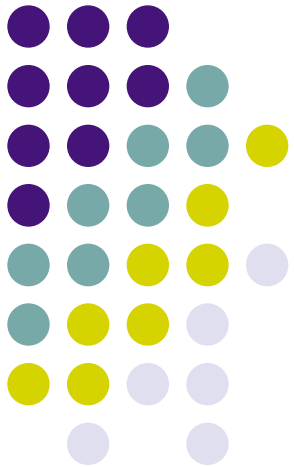
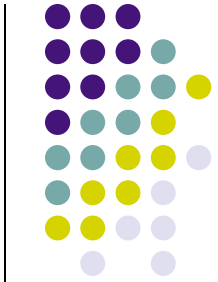
Issues with the MIP6 Security model

I-D: <*draft-patil-mext-mip6issueswithipsec*>

Basavaraj Patil (basavaraj.patil@nokia.com)
Charles Perkins (charliep@wichorus.com)
Hannes Tschofenig (hannes.tschofenig@nsn.com)



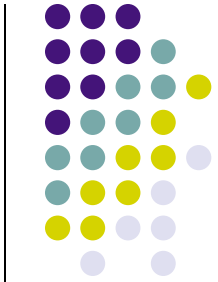
Overview



- Mobile IPv6 (and DSMIP6) rely on IPsec for securing the signaling between the MN and HA

- The tight coupling of the mobility protocol with IPsec is detrimental to broader implementation and deployment

Background



- The choice of IPsec as the security mechanism for MIP6 was based on :
  - the IPv6 design philosophy which intended IPsec as being the IP layer security protocol for other protocols
  - IPsec being an integral part of every IPv6 node

Issues with the use of IPsec by MIP6 (1 of 6)

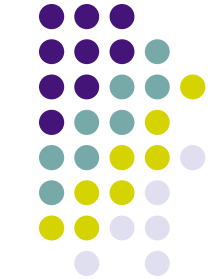
- While the idea of reusing IPsec for mobility signaling may have been sound, IPsec itself is not a good fit for various reasons
  - A MIP6 host implementation must also ensure that IPsec and IKEv2 are part of the stack to begin with – Unnecessary dependency
- Use of IPsec in most hosts today is for VPN connectivity
  - IPsec has not evolved into a generic security mechanism for hosts

Issues with the use of IPsec by MIP6 (2 of 6)

- With IPsec, HA scalability (in terms of number of connections/BCEs) is limited by the number of IPsec SAs that can be terminated

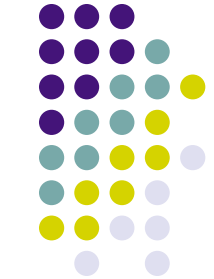
- Implementation complexity: While MIP6 by itself is straightforward to implement on the MN and HA, the interactions that are needed with IPsec and IKEv2 make the protocol unexpectedly difficult

Issues with the use of IPsec by MIP6 (3 of 6)



- It cannot be assumed that every host will have IPsec and IKEv2
  - Coupling MIP6 with IPsec and IKEv2 results in lesser number of hosts supporting IP mobility
- RFC4877 which specifies IKEv2 support for MIP6 basically results in an IPsec variant which is specific to MIP6
  - The reuse value is diminished

Issues with the use of IPsec by MIP6 (4 of 6)



- In many networks alternate security mechanisms for validating the MN/user exist. MIP6 should be able to leverage these means instead of having to mandate another layer of authentication/authorization
- Granularity of selectors that are needed for MIP6 operation was pretty coarse in the past
- Use of IPsec caused undesirable changes to protocol design

Issues with the use of IPsec by MIP6 (5 of 6)

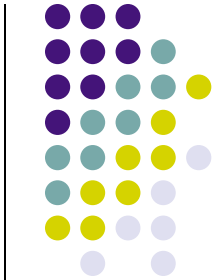
- The way that the IPsec code sits in the usual kernel, and the access mechanisms for the SA database, are not very convenient for use by straightforward implementations of Mobile IPv6. Unusual calling sequences and parameter passing seems to be required on many platforms

Issues with the use of IPsec by MIP6 (6 of 6)

- In certain networks (such as wireless) where the air interface is a valuable resource, IPsec and IKEv2 for MIP6 signaling is viewed as an overhead

If the only tool you have is a hammer….

Conclusion/Proposal



- IPsec/IKEv2 is a drag on MIP6 and will limit the widespread use if it is the only security protocol for securing MIP6 signaling

- If there is consensus on developing a solution to make MIP6 applicability broader, the MEXT WG should charter an alternate design
  - One which is part of the MIP6 protocol itself and does not depend on existence of other mechanisms
  - Reducing the complexity of MIP6 and DSMIP6 is in the interests of the mobility folks in the IETF to ensure real deployments and use