Issues with the use of IPsec/ IKEv2 with MIP6

BASAVARAJ PATIL, CHARLES PERKINS, HANNES TSCHOFENIG AND, DOMAGOJ PREMEC

I-D: draft-patil-mext-mip6issueswithipsec-01

MEXT WG meeting at IETF75

Overview

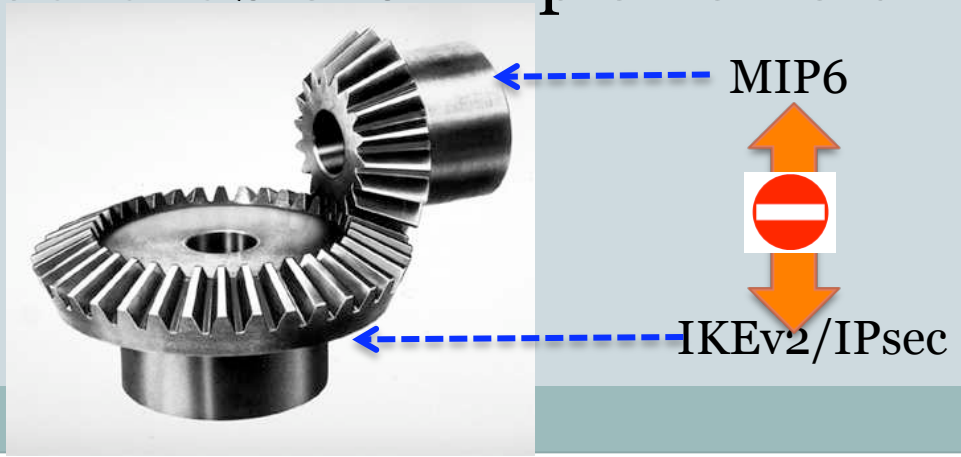
- Mobile IPv6 and consequently DSMIP6 are burdened by their reliance on IPsec/IKEv2 for security

- Implementation issues are discussed in the following slides

Interaction between MIP6 and IKEv2/IPsec

- In the current architecture the IPsec/IKEv2 security subsyetm and (DS)MIP6 module need to interact quite closely for the successful operation of the protocol

- There is no well defined interface between (DS)MIP6 and IKEv2/IPsec available for implementers



Changes to IPsec/IKEv2

- Reuse of the integral security protocol was the primary reason to rely on IPsec/IKEv2
- However in order to implement (DS)MIP6 changes to IKEv2 and in some cases IPsec as well are needed
  - Basically this results in a variant of IPsec/IKEv2 on the host which is specific to (DS)MIP6
- While it is possible to modify the security subsystem in some platforms it is not a given for all OS' and platforms

MIP6 interaction with IKEv2

- MIP6 module needs to trigger IKEv2 to establish an IPsec SA for MIP6 signaling
  - Obtain the HoA as part of the IKEv2 signaling and use the HoA to create the entries in the SPD
- MIP6 module needs to indicate whether it wants the home prefix or the HoA to IKEv2 module
- Basically the point is that the mobility module and IKEv2 modules need to be very tightly coupled
  - Several interfaces such as PF_KEY and MIGRATE have been proposed but none standardized

Issues on the MN and HA

- When the MN configures an address from the HNP (obtained via IKEv2) how does the HA get this address to be used in the SPD creation
  - Does the MN do another IKEv2 exchange to indicate the HoA to the HA for use in the SPD?
- On the MN there is a conflict between whether the key management daemon or the MIP6 module controls and establishes the SPD entry
  - Depending on the host, the MIP6 module again needs to interact with the key management daemon to create the SPD

The “K” bit

- The “k” bit enables the MN to request the key management daemon on the HA to update the end-point address (CoA) as a result of mobility through the BU message
  - Requires again the HA/mobility module to interface with the key management daemon

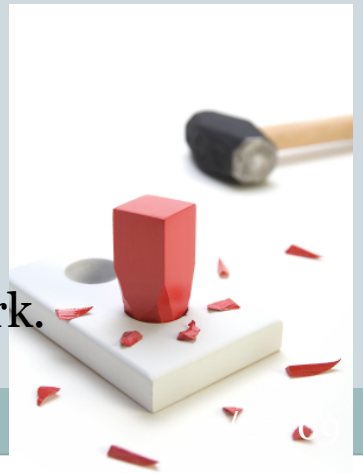
Transport mode SA in DSMIP6

- When the MN is attached to an IPv4 network and behind a NAT, it needs to use only transport mode SA to send a BU to the HA
  - Changes to the IKEv2 module are needed to make this work
- Dealing with NATs in the context of DSMIP6 makes the implementation exponentially more complex than plain MIP6

Summary

- From an implementation perspective, the security framework of IPsec and IKEv2 for (DS)MIP6 on the MN and HA is difficult and complex to code and get it working
- Basically we found that implementing the (DS)MIP6 mobility protocol itself is 10% of the effort and 90% of the time is spent on getting IKEv2 and IPsec integration and changes

MIP6 and IPsec/IKEv2 is equivalaent to trying to put a square peg in a round hole. With enough hammering we can get it to work. But not without some big hammers ☺



Recommendation

- With the current IPsec/IKEv2 as the default security protocol for (DS)MIP6 we don't see this protocol having even a half-chance at seeing any significant implementation and deployment
- Simplifying the security framework would ensure that 10 years or more of work done on this mobility protocol in the IETF does not remain an academic exercise