TLS-based Security solution for Mobile IPv6

draft-korhonen-mext-mip6-altsec-04

Jouni Korhonen,
Basavaraj Patil,
Hannes Tschofenig,
Dirk Kroeselberg

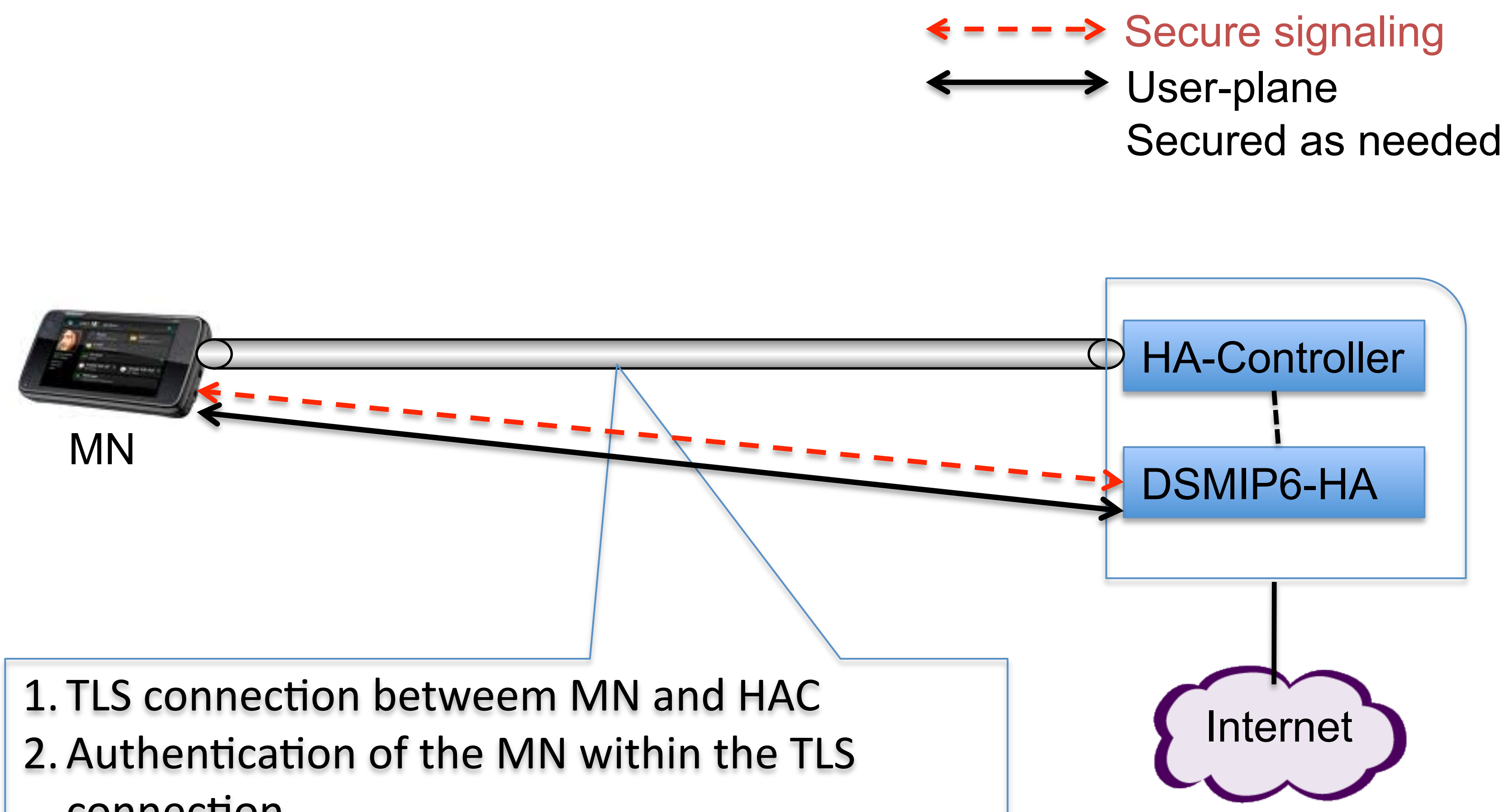
IETF #77, MEXT WG

Background

- Implementing Dual-stack Mobile IPv6 as per RFC5555 using the IKEv2/IPsec based security architecture was an exercise which demonstrated the complexity of integrating IPsec and IKEv2 with Mobile IPv6
- Conclusion that we reached was that DSMIP6 can be significantly simplified by decoupling the protocol from IKEv2/IPsec and replaced with a protocol that provides keys and bootstrapping

TLS based Security architecture

- TLS is a widely implemented and used protocol in the Internet today
- A TLS connection between MN and HA-Controller is established to authenticate the MN and exchange keys as well as bootstrapping information
- Authentication is done within the TLS connection
  - Can be a simple PSK based exchange or
  - With EAP (any EAP method)
- Keys delivered to the MN and HA are used to secure the signaling between MN and HA and user traffic as needed



1. TLS connection betweem MN and HAC
2. Authentication of the MN within the TLS connection
3. Keys delivered to MN and HA for securing the signaling and user-plane traffic
4. Bootstrapping info (v4HoA, v6HoA, HA v4/v6 address, Prefix len) delivered to MN

Status – Changes from 02 -> 03

- Mainly small tweaks that showed up during the implementation exercise..
- Changed the intended status to Experimental.
- Removed the “Mobile IPv6 Service Port number” -> using tbd IANA allocated port.
  - Reason: fixed port easier to handle from firewall management point of view..
- Added version numbering to our “request-response” container protocol.
- Some tweak to IANA considerations and other editorial fixes.

Status – Changes from 03 -> 04

- Blimey.. edited -03 against old version from SVN.. :)
- Basically -04 just reintroduces missing pieces from -02 -> -03 “revision”

Implementation experience (1 of 3)

- Implementation done on Linux (Debian 5)
- Baseline: Building on a DSMIP6 implementation done earlier (2009)
- Implementing the MN-HAC part was quite straightforward and completed
- Used the TLS library in the platform

Implementation experience (2 of 3)

- Implemented EAP-MD5 for user authentication within the TLS tunnel
- Integrating the TLS module with the DSMIP6 MN daemon required some work because of the way the daemon was previously configured to use SPIs and XFRM policies
- Modifying the DSMIP6 MN daemons XFRM code/policies to use UDP encapsulation for signaling and all traffic was the more challenging task

Implementation experience (3 of 3)

- HA-Controller integrated with the HA
- HA changes w.r.t XFRM policies for UDP encap was also the same as the MN

- MN implementation will be made available shortly
- DSMIP6 MN implementation on Nokia N900 in progress

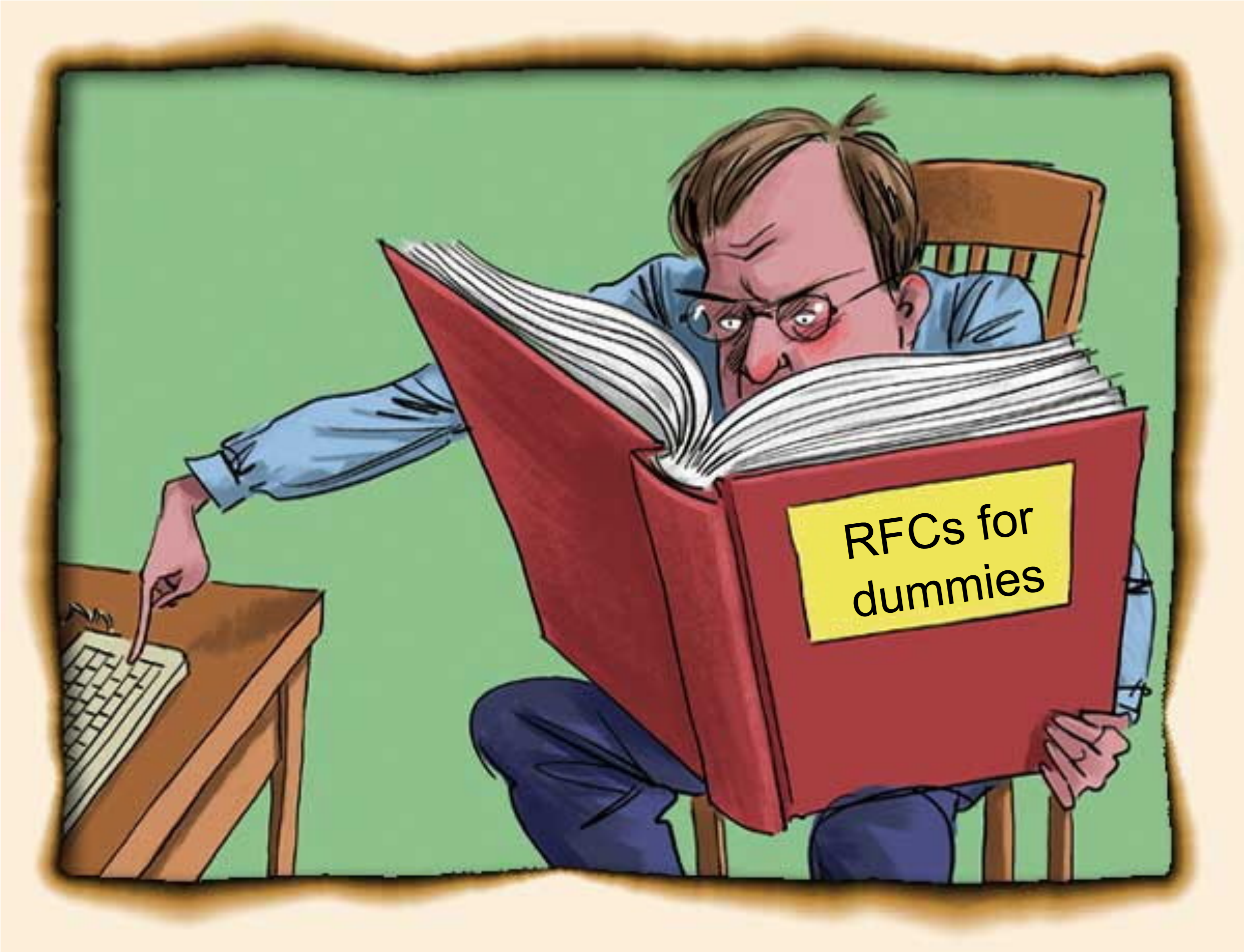
Implementation availability

- DSMIP6 HA using the extensions proposed in draft-korhonen-mext-mip6-altsec will be hosted on nokia.net and made available for interested users (Mid April)
- The MN implementation (Debian 5) will also be made available at the same time
- Contact draft authors for details

Next steps

- Security mechanisms other than IKEv2/IPsec should be specified in order to simplify the protocol
- Request the adoption of this security proposal as an alternative solution for MIP6
- Request I-D adoption as a WG document in MEXT (Experimental)

Questions and Discussion



Picture adapted from Flame Warriors