Use of IPsec with DSMIP

draft-laganier-mext-dsmipv6-ipsec
Julien Laganier

November 2009
IETF-76 (Hiroshima)

Outline

- Architectural Issues
- (DS)MIPv6 vs. IPsec / RFC 4301 Model
- Tunnel Interface Specific SPD Entries
- MN Outbound Processing: new vs. old CoA
- HA Inbound Processing: NAT detection
- Conclusion

Architectural issues

- (DS)MIPv6 processing required both before and after IPsec processing
  - xmit() side:
    - Before IPsec: DSMIPv6 generates MH to be protected by IPsec
    - After IPsec: (DS)MIPv6 encapsulation by, e.g., HoA option substitution, IPv4-UDP encapsulation
  - recv() side:
    - Before IPsec: (DS)MIPv6 decapsulation by, e.g., HoA option removal, IPv4-UDP decapsulation
    - After IPsec: DSMIPv6 processes MH verified by IPsec

(DS)MIPv6 vs RFC 4301 model?

- RFC 3776, 4877 and 5555 lists requirements placed on an IPsec implementation by MIPv6 and DSMIPv6
- These requirements are not necessarily satisfied by a IPsec implementation conformant to RFC 4301
  - Would mean implementing (DS)MIPv6 might requires changes to a conformant IPsec implementation…
- However it seems a conformant RFC 4301 IPsec implementation is sufficient to implement (DS)MIPv6

Tunnel Interface Specific Security Policy Database Entries

- RFC3776 and RFC4877 outline the requirements to have SPD entries that are specific to tunnel interface
- RFC4301 does not mandate interface specific SPD
- Discussion:
  - RFC4301 provides a mean to select traffic based on mobility headers type that makes it possible to use host-wide security policy database entries rather than interface specific SPD entries
  - RFC 4877 tunnel interface selector has been removed from the SPD entry used to specify protection of Return Routability procedure
  - Similarly RFC 4877 SPD entries for protection of payload packets no longer requires to select traffic based on the tunnel interface

DSMIPv6 MN Outbound Processing BUs to new CoA, data to old CoA:

- RFC5555 states:
  - to send the binding update […] the mobile node needs to use the new IPv4 care-of address in the outer header, which is different from the care-of address used in the existing tunnel.
  - DSMIPv6 implementation has to attach additional information to BUs, and this information has to be preserved after IPsec processing and made available to the forwarding function or to DSMIP extensions included in the forwarding function.
- Discussion:
  - SPI in data packets and BUs are different, DSMIP can use this information to infer type of packet and apply appropriate encapsulation

DSMIPv6 HA Inbound Processing: NAT detection BUs

- RFC5555 states:
  - In order to allow the DSMIPv6 implementation in the home agent to detect the presence of a NAT on the path to the mobile node, it needs to compare the outer IPv4 source address with the IPv4 address in the IPv4 care-of address option. This implies that the information in the outer header will be preserved after IPsec processing and made available to the DSMIPv6 implementation in the home agent.
- Discussion:
  - NAT detection occurs at initial attach and after handover
  - Outer IPv4 source address and UDP port is different from those in existing binding cache entries.
  - NAT detection BU can be distinguished based on that, its IPv4 source address and UDP port recorded, and retrieved for BU processing after IPsec processing.

Conclusion

- No change to RFC 4301 nominal processing required to implement (DS)MIPv6