On the Security of the Mobile IP Protocol Family

Ulrike Meyer and Hannes Tschofenig
Nokia Siemens Networks
Germany
Email: ulrike.meyer@nsn.com, hannes.tschofenig@nsn.com

Georgios Karagiannis
University of Twente/CTIT/
The Netherlands
Email: g.karagiannis@utwente.nl

I. Abstract

The Internet Engineering Task Force (IETF) has worked on network layer mobility for more than 10 years and a number of RFCs are available by now. Although the IETF mobility protocols are not present in the Internet infrastructure as of today, deployment seems to be imminent since a number of organizations, including 3GPP, 3GPP2 and Wimax, have realized the need to incorporate these protocols into their architectures. Deployment scenarios reach from mobility support within the network of a single provider to mobility support between different providers and technologies. Current Wimax specifications, for example, already support Mobile IPv4, Proxy Mobile IPv4 and Mobile IPv6. Future specifications will also support Proxy Mobile IPv6. Upcoming specifications in the 3GPP Evolved Packet Core (EPC) will include the use of Mobile IPv4, Dual Stack MIPv6 and Proxy Mobile IPv6 for interworking between 3GPP and non 3GPP networks.

This paper provides an overview on the state-of-the-art in IETF mobility protocols as they are being considered by standardization organizations outside the IETF and focusing on security aspects.

II. The Need for Security

Mobile IP [3], [20] offers a reachability service for mobile nodes (MNs) in which an MN is always identified by the same IP address, namely its home address, regardless of its current point of attachment to the Internet. While away from home a mobile node associates an other IP address, its care-of address with its home address with the help of mobility signalling. The care-of address provides the information about the mobile node's current location. Packets addressed to a mobile node's home address are tunneled to its care-of address. The mobility signaling for this type of communication happens between the mobile node (MN) and the home agent (HA). The details of the mobility signaling procedures are different for IPv4 and IPv6 but the underlying principles are the same. The description in this document focuses mainly on IPv6 since it reflects the more recent development in mobility signaling.

Mobile IPv6 supports establishing a bi-directional tunnel between the MN and the HA such that the traffic between a MN and a CN is routed through the HA in both directions. Alternatively, Mobile IPv6 offers triangular routing and route optimization [3], [21]. In the former case, packets from a MN are directly addressed to the corresponding node (CN) whereas packets in the reverse direction travel through the HA. In the latter case, packets are directly exchanged between the MN and the CN without involving the HA. In order to get this procedure to work there is the need to perform mobility signaling between MN, HA and CN. Although route optimization is preferred from a performance point of view network operators prefer to have a tight control over the data traffic and plan to disable this functionality.

In addition to the basic mobility signaling protocols [3], [20], performance enhancements were developed. An example is Hierarchical Mobile IP (HMIP [22]), which allows signaling and data traffic to be routed locally in the visited network to which the MN is attached as long as MN moves within the visited network. As a consequence, local mobility anchor points had to be introduced into the architecture. Fig. 1 shows all the involved entities. Another example is Fast Handovers for Mobile IP (FMIP [23]), which accelerates the reestablishment of IP connectivity for a moving MN e.g. by establishing a tunnel between the old and new CoA at the access routers in order to overcome the latency of binding updates. So far, these localized mobility schemes have largely a theoretical character.

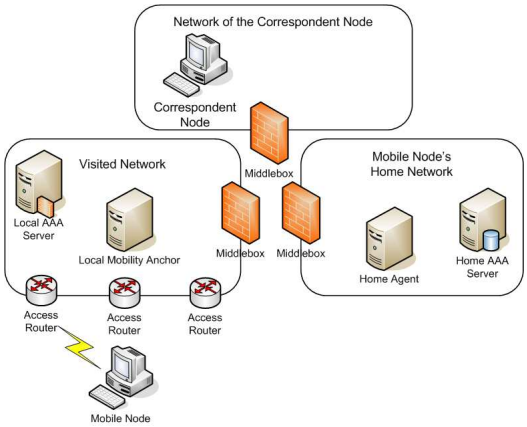

Fig. 1. Entities in the Mobile Internet Architecture

A more interesting trend that evolved in the past few years is shifting the burden of mobility management from the MN to the network and thus performing mobility handling independent of the MN itself. This concept is reflected in Proxy Mobile IP (PMIP [18], [19]). PMIP signaling starts at a node close to the MN (such as the access router) and terminates at a HA. The access router emulates the home network to MN such that the mobility on the IP layer is hidden

from the MN.

With all these mobility signaling protocols that can run between the MN, HA, CN, local mobility anchors and at access routers the classical communication security problems arise: authentication and key establishment between the signaling nodes, integrity protection, replay protection and in some cases confidentiality protection of the signaling traffic.

To provide integrity and replay protection of mobility signaling in MIPv6 between the MN and the HA two approaches were developed; IPsec protection [3] and an approach similar to Mobile IPv4 called MIPv6 Authentication Protocol [6]. For IPsec protection IKEv2 [5] in concert with EAP and Diameter EAP [8] was selected for authentication and key exchange between MN and HA. If the MIPv6 Auth. Protocol is used, then the keys required for integrity and replay protection between MN and HA are derived from keys established between MN and home AAA prior to MIPv6 usage. In Wimax and 3GPP both security approaches are currently under consideration.

Both approaches to secure MIPv6 require the interaction with the AAA infrastructure. This interaction of mobility signaling with the back-end infrastructure also allows to simplify configuration tasks, such as the configuration of Home Agents and Home Addresses, and offers key distribution capability (a feature that is needed for the MIPv6 Authentication Protocol). This work is referred to as Mobile IPv6 bootstrapping [7], [10], and investigates two scenarios: the integrated scenario [24] and the split scenario [4]. In the integrated scenario the network access authentication procedure run between the MN, the AAA client (e.g., access router), local AAA and the home AAA server is used to convey parameters and to establish the keying material for subsequent mobility signaling. This back-end interaction is described in [13], [24]. Conveying the configuration parameters, such as Home Agent address, to the MN happens with the help of DHCP [14]. Subsequently, when the interaction between the MN and the HA takes place the HA still has to interact with the AAA server [4]. In the split scenario there is no such dependency on the network access authentication and the entire bootstrapping procedure is executed between the MN and the HA on the front-end side and between the HA and the AAA server on the back-end side [4]. The back-end infrastructure solutions are available for RADIUS as well as for Diameter and the integrated scenario variant using RADIUS is used in Wimax.

Integrity and replay protection of PMIP signaling between an access router and the HA is based on IPsec. The corresponding security associations are established with the help of IKEv2. An authentication option similar to the one specified for MIPv4 or in the MIPv6 Authentication Protocol [6] is currently not specified for PMIP. The respective interaction with the back-end infrastructure for PMIP is outlined in [17].

III. Conclusion

The specification of the basic mobility signaling protocols including the PMIP protocols can be considered matured. Nevertheless, there are still related open issues to be solved. An example for such an issue is that currently firewalls are typically not aware of MIP-related traffic and therefore interfers with MIP signaling. The problem and some solutions are described in [12], [25], [27]. Another related open issue is location privacy [16], [26]: revealing the care-of address to the CN can reveal location information to the CN and eavesdropping on binding updates can allow an outsider to track the movement of the MN. The work in these problem areas is still ongoing.

References

[1] J. Bournelle et al., *Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction*, Internet draft, work in progress, July 2007.

[2] J. Korhonen et al., *Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction*, Internet draft, work in progress, July 2007.

[3] D. Johnson et al., *Mobility Support in IPv6*, RFC 3775, June 2004.

[4] G. Giaretta et al., *Mobile IPv6 bootstrapping in split scenario*, Internet draft, work in progress, May 2007.

[5] V. Devarapalli et al., *Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture*, RFC 4877, April 2007.

[6] A. Patel et al. *Authentication Protocol for Mobile IPv6*, RFC 4285, January 2006.

[7] A. Patel et al., *Problem Statement for bootstrapping Mobile IPv6 (MIPv6)*, RFC 4640, September 2006.

[8] P. Eronen et al., *Diameter Extensible Authentication Protocol (EAP) Application*, RFC 4072, August 2005.

[9] C. Kaufman, *Internet Key Exchange (IKEv2) Protocol*, RFC 4306, December 2005.

[10] G. Giaretta et al., *AAA Goals for Mobile IPv6*, Internet draft, work in progress, September 2006.

[11] K. Chowdhury et al. *MIP6-bootstrapping for the Integrated Scenario*, Internet daft, work in progress, June 2007.

[12] F. Le et al. *Mobile IPv6 and Firewalls: Problem Statement*, RFC 4487, May 2006.

[13] K. Chowdhury, et al. *RADIUS Mobile IPv6 Support*, Internet draft, work in progress, March 2007.

[14] H. Jang, et al. *DHCP Option for Home Agent Discovery in MIPv6*, Internet draft, work in progress, May 2007.

[15] H. Soliman, et al., *Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)*, July, 2007.

[16] R. Koodli, *IP Address Location Privacy and Mobile IPv6: Problem Statement*, RFC 4882, May 2007.

[17] J. Korhonen, et al., *Diameter Proxy Mobile IPv6: Support For Mobility Access Gateway and Local Mobility Anchor to Diameter Server Interaction*, Internet draft, work in progress, June, 2007.

[18] S. Gundavelli, et al., *Proxy Mobile IPv6*, Internet draft, work in progress, September, 2007.

[19] K. Leung, et al., *WiMAX Forum/3GPP2 Proxy Mobile IPv4*, Internet draft, work in progress, July, 2007.

[20] C. Perkins, *IP Mobility Support for IPv4, revised*, Internet draft, work in progress, July, 2007.

[21] P. Nikander, et al., *Mobile IP Version 6 Route Optimization Security Design Background*, RFC 4225, December 2005.

[22] H. Soliman, et al., *Hierarchical Mobile IPv6 Mobility Management (HMIPv6)*, RFC 4140, August, 2005.

[23] R. Koodli, *Fast Handovers for Mobile IPv6*, Internet draft, work in progress, July 2007.

[24] K. Chowdhury, et al., *MIP6-bootstrapping for the Integrated Scenario*, Internet draft, work in progress, June 2007.

[25] S. Krishnan, et al., *Firewall Recommendations for MIPv6*, Internet draft, work in progress, June 2007.

[26] Y. Qiu, et al., *Mobile IPv6 Location Privacy Solutions*, Internet draft, work in progress, May 2007.

[27] H. Tschofenig, et al., *Mobile IP Interactive Connectivity Establishment (M-ICE)*, Internet draft, work in progress, July 2007.