Re-thinking Security in Network Mobility

Jukka Ylitalo, Ericsson Research NomadicLab *

Abstract

Once a router changes its topological attachment to the Internet, end-hosts attached to the subnetwork behind the router become temporarily unreachable. As a result, the end-hosts cannot sustain their connections without some kind of mobility support. To mitigate this problem, several existing approaches apply end-host mobility protocols to network mobility issues. However, the currently proposed approaches implement triangular routing without scalable support for nested mobile networks. They also suffer from packet size overhead, caused by extra tunneling headers.

In this paper, we present a scalable and secure network mobility infrastructure based on the Host Identity Protocol (HIP). We use public-key based host identifiers to delegate mobility signaling rights from end-hosts to mobile routers. As a result, we obtain a network mobility infrastructure supporting IPsec, route and signaling optimization, and nested mobile networks.

KEYWORDS: Network Mobility, Signaling Delegation, Signaling optimization, Security

1 Introduction

Our secure network mobility approach is based on the Host Identity Protocol (HIP)[6] and its public-key based name space. Each host, including *mobile hosts (MHs)* and *mobile routers (MRs)*[4], is identified with a cryptographic *host identifier (HI)* [6]. A *locator*, i.e., an IP address, defines the topological point-of-attachment of HI to the network. As a result, the end-to-end transport layer connections are bound to HIs, instead of IP addresses. Furthermore, the HIs are dynamically bound to locators at a new logical layer between the transport and IP layers. The dynamic one-to-many binding between HIs and locators provides simultaneously mobility and multi-homing properties both for MHs and MRs. In our architecture, mobile routers are authorized by mobile hosts to update the binding between mobile hosts' HIs and their locators at the peer hosts.

In our approach, HI enabled Network Address Translation (NAT) solves the address assignment problems related to nested mobile networks. The HI enabled NAT translated IP addresses and acts as a router for HIs. As IPsec is used, the IPsec Security Parameter Index (SPI) values work as indices for HIs. A mobile router learns the SPIs together with the HIs during the initial end-to-end key exchange or from any subsequent mobility signaling [12]. In practice, each mobile router implements SPI multiplexed NAT (SPINAT)[13], working like a NAPT[7], but for SPI values. [1]

*Tel. +358 400 615821, fax. +358 9 299 3535, email: Jukka.Ylitalo@nomadiclab.com

2 Signaling Delegation Infrastructure

Each MR implements four different functionalities; acting as an access router, a SPINAT device [13], a micro-mobility anchor point[12], and a mobility signaling proxy for MHs and other nested MRs. The address assignment is a key issue when trying to obtain fast hand-offs and scalable nested mobile networks. Therefore, SPINAT plays a key role in our architecture. However, the biggest optimization is obtained with the signaling proxy functionality[8] that minimize the signaling traffic over the air and offers route optimization functionality between the mobile routers and end-hosts.

2.1 Address Assignment

Once a MH attaches to a mobile network, the MR assigns *a local unicast address* [9] to the MH. The MH and MR learn the HIs of each other during an enhanced Secure Neighbor Discovery[10] exchange or DHCP(v6)[11] lease [2]. The MH may delegate mobility signaling rights to the MR already during this link local exchange.

In the nested MR moving network case, each MR works as an access router for another MR in the hierarchy. The MR hides network mobility from the MHs and other nested MRs attached to its local link. Once the MR makes a hand-off, it takes care about the mobility signaling on behalf of the MHs and MRs attached to it. From the MH point of view, the MR works also as a Mobile Anchor Point (MAP) hiding the micro-mobility from the peers [12].

[1] The security considerations of SPINAT are discussed in [13].

[2] The exact definitions of HI enhanced link local exchanges are out of this paper's scope.

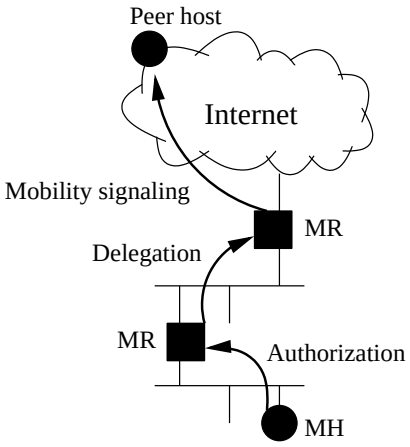

Figure 1: Signaling delegation.

2.2 Signaling Proxy

The signaling delegation is based on the Simple Public Key Infrastructure (SPKI) that defines an authorization mechanism between public-key pairs. An authorization certificate consists of the following five-tuple:

$$< Issuer, Subject, Delegation, Tag, Lifetime >$$

In our approach, HIs name the issuer and the subject. In the network mobility case the subject is also called *a signaling proxy*. The MH delegates mobility signaling rights to the MR. In most cases, the issuer also allows the subject to further delegate the rights. Therefore, in the nested MR case, a MR may delegate signaling rights to another MR connected to the Internet, as illustrated in Figure 1. Finally, the edge MR may even delegate the signaling rights to a signaling proxy locating in the Internet.

The architecture defines a single authorization tag, i.e., an *update* tag, allowing the subject to send address binding updates on behalf of the issuer. The lifetime of the certificate is the expected stay of the issuer at the current location. The latest certificate signed by the issuer revocates all the earlier signed certificates by the same issuer. In this way, the peer host only accepts messages with the latest timestamp.

Each MH in the mobile network authorizes its access router to send address binding updates to the peer hosts. After the initial authorization, it is enough that the the signaling proxy sends a single address binding update per peer host. This is an important optimization, because several MHs may be connected to the same peer host. If the edge MR has delegated the signaling rights to a Mobile Anchor Point (MAP)[12] in the Internet, the saving in the over-the-air signaling is enormous. Basically, it is enough that after the initial authorization exchange the edge MR sends a single message to the signaling proxy in the core network that takes care of sending the address binding updates to the peer hosts.

3 Conclusions

We have shortly presented a secure NEMO like architecture protecting hosts from attacks presented by Aura et.al. in [5]. The solution reduces the amount of over-the-air signaling in the mobile network and between the mobile network and the Internet. The signaling optimization is based on the signaling rights delegation between hosts using public key based host identifiers. A signaling proxy may send address binding updates to the peer host on behalf of its clients. The signaling proxy may locate at the mobile router or in some micro-mobility supporting node in the Internet. The packets are routed directly between the mobile router and the peer hosts. The architecture supports also nested mobile networks by implementing overlay routing for HIs with SPINAT functionality. Interested readers may look at related work, including Delegation-Oriented Architecture (DOA)[1] and network mobility work, e.g., [4][2][3].

References

[1] Walfi sh, M., et.al. Middleboxes No Longer Considered Harmful. In *Proc. USENIX OSDI*, San Francisco, CA, Dec., 2004.

[2] Wakikawa, R., et.al. Demonstration System supporting Host and Network Mobility. Symposium on Multimedia, Distributed, Cooperative and Mobile Systems (DICOMO), Akan Lake Hokkaido, Japan, June 2003.

[3] Mitsuya, K., Uehara, K., Murai, J. The In-vehicle Router System to Support Network Mobility. ICOIN2003, vol.2, page. 890-899, Jeju Island, Korea, February 2003.

[4] Ernst, T. Network Mobility Support in IPv6. Doctoral thesis. Department of Mathematics and Computer Science. Universite Joseph Fourier. France. Oct. 2001.

[5] Aura, T., Roe, M., Arkko, J. Security of Internet Location Management. In *Proc. Asia-Pacific Computer Systems Architecture Conference, ACSAC'02*. Monash University, Melbourne, Australia. Feb. 2002.

[6] Nikander, P., Ylitalo, J., Wall, J. Integrating Security, Mobility, and Multi-Homing in a HIP Way. In *Proc. Network and Distributed Systems Security Symposium (NDSS'03)*. Feb. 2003.

[7] Srisuresh, P. Holdrege, M. IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663. 1999.

[8] Nikander, P., Arkko, J. Delegation of Signalling Rights. In *Proc. of the Security Protocols, 10th International Workshop*, Cambridge, UK, April 16-19, 2002, LNCS 2845, pp. 203-212, Springer, 2003.

[9] Hinden, R., Haberman, B. Unique Local IPv6 Unicast Addresses. Internet-draft. Work in progress. Oct. 2004.

[10] Nikander, P., Kempf, J., Nordmark, E. IPv6 Neighbor Discovery (ND) Trust Models and Threats. RFC 3756. May 2004.

[11] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., Carney, M. Dynamic Host Confi guration Protocol for IPv6 (DHCPv6). RFC 3315. July 2003.

[12] Ylitalo, J., Melén, J., Nikander, P., Torvinen, V. Rethinking Security in IP based Micro-Mobility. In *Proc. of the 7th Information Security Conference (ISC'04)*. pp. 318-329, Palo Alto, CA, USA, Sep. 2004.

[13] Ylitalo, J., Salmela, P., Melén, J., Tschofenig, H. Integrating IPsec into the Internet Indirection Infrastructure. submitted to European Wireless 2005.