Network Working Group
Internet-Draft
Expires: December 10, 2006

Y. El Mghazli
Alcatel
J. Bournelle
GET/INT
J. Laganier
DoCoMo Euro-Labs
June 8, 2006

MPA using IKEv2 and MOBIKE
draft-yacine-preauth-ipsec-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 10, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document describes how to achieve media-independent pre-authentication (MPA) in the context of network accesses protected by IPsec. In such environments, access is protected by an IPsec tunnel mode security association (SA) established between a client of the network and an access gateway. This SA normally needs to be

established by running an IKE exchange between the two SA endpoints. The duration of this IKE exchange make it impractical to use when the node is mobile and frequently change either its location or its access gateway during a handover. In most case it is expected that real time traffic will be impacted by the handover. This note describes a method that alleviate this issue by leveraging on the IKEv2 Mobility and Multihoming Protocol (MOBIKE). The described method supresses the need to run a full IKE exchange after each handover, thereby greatly reducing the impacts of handovers on real-time traffic.

Table of Contents

1. Terminology and Definitions

Most of the terms are extracted from [I-D.ohba-mobopts-mpa-framework] and [I-D.ietf-mobike-protocol].

Media-independent Pre-Authentication Mobile Node (MN):

A mobile terminal of media-independent pre-authentication (MPA) which is a mobile-assisted, secure handover optimization scheme that works over any link-layer and with any mobility management protocol. An MPA mobile node is an IP node. In this document, the term "mobile node" or "MN" without a modifier refers to "MPA mobile node". An MPA mobile node usually has a functionality of a mobile node of a mobility management protocol as well.

Candidate Target Network (CTN):

A network to which the mobile may move in the near future.

Gateway (GW):

In this document, a Gateway is an Access Router using IKEv2.

IPsec TIA

Inner Address of the IPsec Tunnel.

IPsec TOA

Outer Address of the IPsec Tunnel.

Target Network (TN):

The network to which the mobile has decided to move. The target network is selected from one or more candidate target network.

Proactive Handover Tunnel:

A bidirectional IP tunnel that is established between the MPA mobile node and an access router of a candidate target network. In this document, the term "tunnel" without a modifier refers to "proactive handover tunnel".

Care-of Address:

An IP address used by a mobility management protocol as a locator of the MPA mobile node.

2. Introduction

2.1. Media Pre-Authentication Framework

One of the current goal in IP based network is to achieve seamless handover. While it exists solutions at layer 2 or IP level, the authentication process is most of the time not considered. The document [I-D.ohba-mobopts-mpa-framework] introduces a framework to achieve this goal by relying on pre-authentication. This means the mobile authenticates to a candidate target network before attaching to it.

The proposed framework is the following (extracted from [I-D.ohba-mobopts-mpa-framework]):

1. The Mobile establish a Security Association with a Candidate Target Network (CTN) to secure subsequent protocol signalling.

2. It securely executes a configuration protocol to obtain an IP address and other parameters from the CTN.

3. It executes a tunnel management protocol to establish a Proactive Handover Tunnel (PHT) (i.e. a bidirectionnal tunnel between the MN and an access router of the CTN).

4. Through this PHT, the MN can send and receives IP packets including signaling messages for the Mobility Management Protocol. As a consequence, it can receives IP data packets resulting from this new binding.

5. Finally, it deletes or disables the PHT immediatly before attaching to the CTN. Then it reassigns the inner address of the PHT to the physical interface immediatly after the MN is attached to the CTN.

In this document, we propose a solution for MPA based on IKEv2 and MOBIKE.

2.2. IKEv2 and MOBIKE overview

2.2.1. IKEv2

The IKEv2 protocol [RFC4306] mutually authenticate two peers (named Initiator and Responder) in order to dynamically and securely establish IPsec SAs. It can be divided in two main phases. In the first phase called IKE_SA_INIT, the two peers establish an IKE SA (Security Association) to protect subsequent messages. In the second phase, called IKE_AUTH, the two peers authenticate each other and

start to configure IPsec SAs. If others IPsec SAs are needed, they use the CREATE_CHILD_SA exchange which relies on previous authenticated IKE SA.

The two main features of interest for this document are:

1. The IKEv2 specification allows the Responder to authenticate Initiator by using the EAP protocol [RFC3748]. This permits to the Responder to rely on a AAA server to authenticate the Initiator. Note that Initiator authenticates the responder based on public-key based mechanism.

2. The IKEv2 allows to establish an IPsec tunnel between the Initiator and the Responder to protect data traffic.

2.2.2. MOBIKE

The MOBIKE protocol [I-D.ietf-mobike-protocol] is an extension of IKEv2. It allows to change an IP address associated with IKEv2 and an IPsec tunnel to change without reusing IKEv2 from scratch. This feature is particulary useful to achieve an efficient MPA with IKEv2.

2.3. IPsec protection in the access network

In such environments, access is protected by an IPsec tunnel mode security association (SA) established between a client of the network and an access gateway. This SA normally needs to be established by running an IKE exchange between the two SA endpoints. The duration of this IKE exchange make it impractical to use when the node is mobile and frequently change either its location or its access gateway during a handover. In most case it is expected that real time traffic will be impacted by the handover.

Examples of access networks typically protected by IPsec are 3G/WLAN interworking technologies, namely UMA [UMA] and I-WLAN [I-WLAN].

3. MPA with IKEv2 and MOBIKE

This document describes a method to achieve media-independent pre-authentication (MPA) in the context of network accesses protected by IPsec. This method alleviates the issues of long delays involved with running a complete IKE exchange after handover by leveraging on the IKEv2 Mobility and Multihoming Protocol (MOBIKE). It does so by supressing the need to run a full IKE exchange after each handover, thereby greatly reducing the impacts of handovers on real-time traffic.

The solution is to pre-establish a pre-handover IPsec tunnel mode (PHT) SA with the access gateway; When a handover occurs, the mobile node use MOBIKE to update the outer address of the tunnel, thereby transforming the PHT into a regular Access Tunnel.

Thus, combining MOBIKE and Pre-Authentication allows in this context to reduce the overall IP connectivity re-establishment delay to the L2 handoff only.

The MPA framework considers the 3 following entities:

1. The Authentication Agent: this entity is responsible of the pre-authentication.

2. The Configuration Agent: this entity is responsible to securely deliver an IP address and other configuration parameters to the mobile node.

3. The Access Router: It is the router with which the Mobile Node establishes a proactive handover tunnel.

In the proposed approach, the three following functionalities are handled by the IKEv2 Responder colocated with the Access Router.

3.1. First Step: IKEv2 pre-authentication

Initially, the Mobile Node obtains IP connectivity in a access domain. Thanks to a mechanism out-of scope of this document, the Mobile Node discovers a new GW to which it may attach.

It starts a pre-authentication procedure with this nGW using IKEv2.

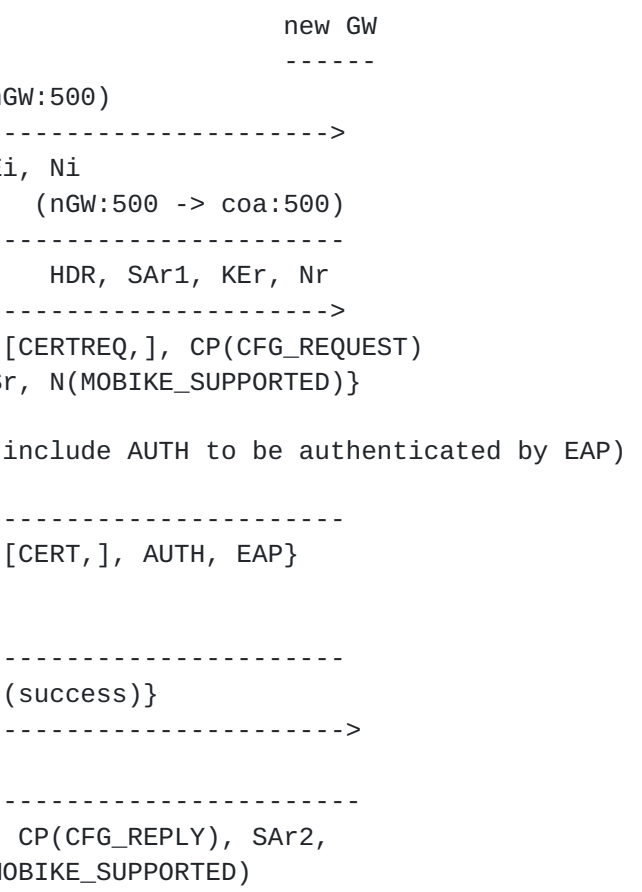
This IKEv2 preauthentication procedure has the following goals:

- Establish an IPsec tunnel between MN and the nGW.

o Obtains an address valid in the Candidate Target Network. This is achieved thanks to CFG_REQUEST/CFG_REPLY of IKEv2.

This address will be be attached to the physical interface after the Mobile Node attaches to the new access network. As a consequence, after attachment, this new address will be used as the outer address of the tunnel between MN and the nGW and thus must be valid in the new visited access network.

The following IKEv2 messages are exchanged between MN and the nGW. These exchanges occur while the Mobile Node is still in the previous access network.



After IKEv2 preauthentication, the Mobile Node has an IPsec tunnel with the nGW.

The IPsec tunnel with nGW has the following header:

o IPsec TOA: CoA and nGW

o IPsec TIA: nCoA and Correspondent Node

This IPsec tunnel corresponds to the secure Proactive Tunnel. The Mobile Node can use its Mobility Management Protocol inside this tunnel to indicate its future new location (nCoA).

When the MN changes of visited network, the source outer adress is no longer valid. The next section explains how MOBIKE can be used to achieve an efficient handover.

The new GW has allocated the nCoA for the Mobile Node which is not yet in its access network. However, it knows that the Mobile Node is supposed to come in its access network.

At this point of time, it is not clear if the Mobile Node must indicate in this IKEv2 exchange that it is a pre-authentication.

3.2. Completing MPA with MOBIKE

As a result of the IKEv2 preauthentication with nGW, the Mobile has an IKE_SA with the nGW. However, the source outer address of the IPsec tunnel is not valid in nGW's access network. To avoid a complete reauthentication procedure with nGW, we propose to use the MOBIKE protocol.

For this purpose, the Mobile Node sends an INFORMATIONAL IKEv2 messages containg an UPDATE_SA_ADDRESSES:

```
Mobile Node                nGW
-----------                -----------
 HDR, SK { N(UPDATE_SA_ADDRESSES),
           [N(NAT_DETECTION_SOURCE_IP),
            N(NAT_DETECTION_DESTINATION_IP)],
           [N(NO_NATS_ALLOWED)],
           [N(COOKIE2)] } -->
```

Note that this packet is sent right after the Mobile Node has performed its IP handover and as such the Mobile Node uses its nCoA as source IP address.

As it is the nGW which has allocated this nCoA, it can validate this request. Then it updates its IKE_SA with the IP address of the IP header of the IKEv2 message. It replies with an IKEv2 INFORMATIONAL message and finally it updates the IPsec SAs associated with this IKE_SA with the new addresses.

If the MOBIKE exchange is successfull, the Mobile Node now has the

following tunnel with the nGW:

- IPsec TOA: nCoA and nGW
- IPsec TIA: nCoA and CN

This optimized approach recycles the PHT as the IPsec tunnel, which protects the data flows in an IPsec-protected access environment. This avoids the need to re-authenticate with the nGW and re-establish an IPsec tunnel for this purpose.

4. Security Considerations

The security considerations on this proposal need to be further studied. However, because the proposal uses unmodified IKEv2 and MOBIKE protocols in the context of pre-authentication with IPsec protected network accesses, it is believed by the authors that the proposal does not introduce any additional threats neither to the existing IKEv2 and MOBIKE protocols, nor to the architecture which relies on them for network access authentication (e.g. 3GPP IWLAN, UMA).

5. IANA Considerations

This document has no IANA considerations.

6. Acknowledgements

The authors would like to thank Maryline Laurent-Maknavicius and Olivier Marce for useful discussions on this topic.

7. References

7.1. Normative References

[I-D.ietf-mobike-protocol]
Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", draft-ietf-mobike-protocol-08 (work in progress), February 2006.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

7.2. Informative References

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[I-D.ietf-mobike-design]
Kivinen, T. and H. Tschofenig, "Design of the MOBIKE Protocol", draft-ietf-mobike-design-08 (work in progress), March 2006.

[I-D.ohba-mobopts-mpa-framework]
Ohba, Y., "A Framework of Media-Independent Pre-Authentication (MPA)", draft-ohba-mobopts-mpa-framework-02 (work in progress), March 2006.

[I-D.ohba-mobopts-mpa-implementation]
Ohba, Y., "Media-Independent Pre-Authentication (MPA) Implementation Results", draft-ohba-mobopts-mpa-implementation-02 (work in progress), March 2006.

[I-D.ohba-mobopts-heterogeneous-requirement]
Dutta, A., "Problem Statement for Heterogeneous Handover", draft-ohba-mobopts-heterogeneous-requirement-01 (work in progress), March 2006.

[I-D.ietf-pana-preauth]
Ohba, Y., "Pre-authentication Support for PANA", draft-ietf-pana-preauth-01 (work in progress), March 2006.

[I-WLAN] 3GPP, "3GPP system to Wireless Local Area Network (WLAN) interworking; System description", TS 23.234, December 2005.

[UMA] UMA technology, "Unlicensed Mobile Access", Stage 2 Specifications R1.0.4, May 2005.

Authors' Addresses

Yacine El Mghazli
Alcatel
Route de Nozay
Marcoussis 91460
France

Email: yacine.el_mghazli@alcatel.fr

Julien Bournelle
GET/INT
9, rue Charles Fourier
Evry 91011
France

Email: julien.bournelle@int-evry.fr

Julien Laganier
DoCoMo Communications Laboratories Europe GmbH
Landsberger Strasse 312
Munich 80687
Germany

Phone: +49 89 56824 231
Email: julien.ietf@laposte.net
URI: http://www.docomolab-euro.com/

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.