Mobile IP Working Group
INTERNET-DRAFT
Expires: February 2002

Hesham Soliman, Ericsson
Karim El Malki, Ericsson
Tomas Goldbeck-Lowe, Ericsson
July, 2001

Security Association establishment for Mobile IPv6 Route Optimisation using AAA

<draft-soliman-mobileip-routeopt-mipv6-02.txt>

Status of this memo

Abstract

This draft describes a simple mechanism that allows a MN to establish a security association with a CN to enable it to send Binding Updates in a secure manner as required by MIPv6. The proposed mechanism makes use of the AAA infrastructure and is only intended for securing network signalling data (e.g. BU's from MN) but not traffic. It should be noted that the use of this mechanism need not be limited to MIPv6 BUs and may be utilised to allow any two nodes to setupa security asociation using the AAA infrastructure.

TABLE OF CONTENTS

1. Introduction

MIPv6 provides a powerful and flexible way of optimising a route between a MN and a CN based on an end-to-end approach. Route optimisation is required to reduce the delays in packet arrivals between a CN and a MN. Such delays may be significant, depending on the number of hops in the path MN-HA-CN and the level of congestion in such path. Route optimisation is achieved when a MN sends a Binding Update (BU) to a CN. According to [MIPv6], BUs MUST be secured by at least an Authentication Header [AH]. Security association establishment between a MN and a CN requires that the MN and CN have some authorisation credentials (e.g. certificates) and a mechanism to establish SAs which includes key exchange. One possible key exchange mechanism is explained in [IKE].

The aim of this draft is to introduce a simple mechanism based on the AAA infrastructure that allows key generation and distribution for securing BUs between a MN and a CN. The proposed mechanism relies on the existing trust models within a AAA infrastructure, hence resulting in less messages required to exchange keys between a MN and a CN than for example IKE requires. This will reduce connection setup latencies as well as the overhead (i.e. number of messages) required for security association establishment. Such enhancements are especially relevant to real time services and wireless networks where radio links have strict requirements on bandwidth efficiency. Furthermore, since the proposed mechanism assumes an existing level of trust within the AAA infrastructure, the required protocol would be relatively simple to implement.

In the proposed AAA model, the AAA servers/clients within one network domain share a security association, e.g. a AAA client in an attendant node have a SA with the AAA server in the same network. All traffic between these entities are authenticated using this SA. Also, AAA servers in different domains share the same type of SA as part of the roaming agreement.

It should be noted that the proposed mechanism is not intended to replace key exchange mechanisms (e.g. IKE, KINK) aimed at generic SA establishment between two nodes. The mechanism described in this draft mainly addresses SA establishment for the needs of MIPv6 signalling between MN and a CN which belong to networks supporting AAA. When using the proposed mechanism in this draft, the home AAA servers will be aware of the SA between the MN and the CN. This mechanism will therefore provide sufficient security for MIPv6 BUs only under the assumption that the owners of the AAA home servers (i.e. the operators which the MN and CN trust and have a subscription to) have no interest in disrupting the communication of their customers.

Finally, by using this mechanism, the authorisation issues for accepting a BU from a MN will be resolved.

2. Limitations

The mechanism proposed in this draft only applies when both the MN and the CN are connected to the AAA infrastructure. This means that hosts that do not rely on the AAA infrastructure, can not use this method. The CN may be a fixed or mobilie host,router, or server.

3. Establishing Security Associations

3.1 Initial assumptions and limitations

Since no AAA protocol has been decided upon yet to authenticate an IPv6 user to the network, some assumptions are made about the services that will be provided by the AAAv6 protocol. These assumptions may be used by developers as requirements on AAAv6.

In this memo, the communication between the MN and AAAL is not assumed to use the same protocol as the AAA-AAA servers communication protocol. This allows for some flexibility for the MN-AAA protocol choice. Also, direct communication between the AAA and the MN is an option but it is NOT mandated, even though the figures may indicate that. A node in between, often referred to as attendant, should be allowed. If the attendant is present, it will handle the translation from the IPv6 host protocol to the AAA server protocol.

Since no method currently exists to allow route optimisation between IPv6 and IPv4 hosts, IPv6 MNs will not be able to use this method when communicating with IPv4 hosts.

The key request message will be defined as extensions to both the host-AAA server protocol and the AAA-AAA server protocol. That will allow all servers to identify the request as a key request for binding updates between the specific MN and CN.

3.2 Operational overview

The model proposed for establishing a Security Association is illustrated below in Fig. 1. The communication between the MN and the CN is divided into two separate protocols: the IPv6 host-AAA server protocol and the AAA-AAA server protocol. Messages received from IPv6 hosts by the attendant or local AAA server are translated and forwarded to the other host's AAA server. It should be noted that the model shown below need not be limited to security associations between IPv6 hosts. The same model can be used to establish security associations between IPv6 hosts and IPv6 routers, provided they have pre-established security associations with their respective AAAH servers.

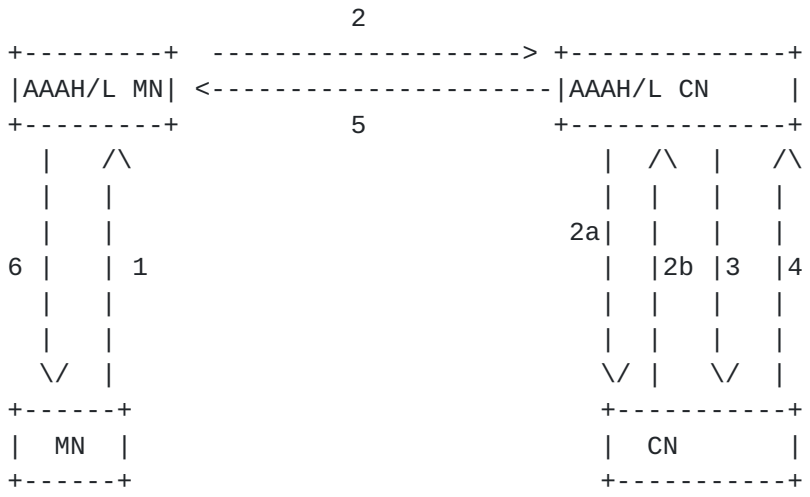

Figure 1. Basic model

A MN may request another entity, with which it has a pre-established trust (i.e. AAAH-MN), to set up a security association between the MN and another CN for securing BU messages. The request can be sent to the AAAL which in turn relays it to AAAH for the MN. Alternatively the MN can send the request directly to AAAH-MN.

The information passed from the MN to the AAAL/AAAH server (message 1 above) should contain the following:

- Message authentication based on MN-AAAH Security Association.
- MN's Home Address and NAI.
- IPv6 address or NAI for the CN.
- Security algorithms supported by the MN.
- Lifetime requested for the generated security association.

Users must be forbidden from using, for the SA establishment procedure, home IP addresses which cannot be authenticated/authorised by the AAAH. Therefore the AAAH MUST reject an SA establishment request (message 1) which contains a MN home address/NAI and does not provide the appropriate message authentication based on the MN-AAAH shared secret. This assumes the Mobile IP model where the MN has a pre-shared secret with its home network.

The request is forwarded from AAAL to AAAH (in case the MN is in a foreign domain). The request MUST be secured by using the AAAL-AAAH security association.

Upon reception of the request from the MN, AAAH needs to locate the AAAH-CN. The request is then forwarded to the AAAH-CN. This is shown as step 2 in the figure above.

Upon reception of the request by the AAAH-CN, a decision is made as to whether a key is generated immediately or after consulting the CN.

The decision is based on the AAA server's knowledge of the CN. For example, a CN may have a certain profile in the AAA server that allows it to make such decision based on the CN's security preferences. Otherwise the CN is consulted first as shown in Fig. 1 by sending message 2a. The message contains all the information given by the MN. The contents of the message should be validated by the CN and result in sending a reply message 2b. It should be noted that the messages 2a and 2b are optional and may not be sent if the AAAH-CN has the necessary information about the MN.

If the CN agrees to set up a security association it should include a supported algorithm and a lifetime value for the security association. Otherwise a rejection is sent with the appropriate error code. It should be noted that the key generated may not have the same lifetime value as the one requested by the MN.

Upon reception of an acceptance from the CN, or a positive decision taken directly by the AAAH-CN based on the CN profile, the AAAH-CN should generate the key and send it to the CN (message 3) and to the AAAH-MN. The CN should reply to the AAAH-CN with an acknowledgement. After this, the key is also sent to the AAAH-MN.

It should be noted that it is possible that the communication between AAAH-CN and the CN is done via AAAL while the CN is outside the AAAH-CN domain. In this case AAAH-CN should have knowledge of the CN's current AAAL. This knowledge can be stored while authenticating the CN to the foreign domain and is within the scope of the AAAv6 work.

Finally, the reply is relayed by the AAAH-MN to the MN via AAAL or directly.

In the case where the MN is located in the AAAH-MN domain, the MN should send the request directly to AAAH-MN. The MN should use its MN-AAAH session key for communicating with AAAH.

4. Acknowledgements

The basic concepts behind this draft were discussed between the authors, Annika Jonsson and Martin Korling. We would like to thank them for their input. The authors would also like to thank Pekka Nikander (Ericsson) for his valuable feedback.

5. References

[MIPv6] D. Johnson and C. Perkins, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-12.txt, February 2000.

[IKE] D. Harkell and D. Carrel, "The Internet Key Exchange", RFC 2409.

[AH] S. Kent and R. Atkinson, "IP Authentication Header", RFC 2402.

7. Authors' addresses

Hesham Soliman
Ericsson Australia
61 Rigall St., Broadmeadows
Melbourne, Victoria 3047
AUSTRALIA

Phone: +61 3 93012049
Fax: +61 3 93014280
E-mail: Hesham.Soliman@ericsson.com.au

Karim El Malki
Ericsson Radio Systems AB

LM Ericssons Vag. 8
126 25 Stockholm
SWEDEN

Phone: +46 8 7195803
Fax: +46 8 7190170
E-mail: Karim.El-Malki@era.ericsson.se

Tomas Goldbeck-Lowe
Ericsson Radio Systems AB
Networks and Systems Research
SE-164 80 Stockholm
SWEDEN

Phone: +46 8 764 1467
Fax: +46 8 404 7020
E-mail: Tomas.Goldbeck-Lowe@era.ericsson.se