Mobile IP WG
INTERNET-DRAFT
Date: 23 February 2001
Expires: 23 August 2001

Franck Le
Stefano M. Faccin
Nokia Research Center

Key distribution mechanisms for Mobile IPv6
<draft-le-mobileip-keydistribution-00.txt>

Status of This Memo

Abstract

Mobile IP and many of its extensions such as Mobile IPv6 Regional Registration [1] or Hierarchical MIPv6 Mobility Management [2] require strong authentication between the mobile node and different agents (Home Agent, Gateway Mobility Agent [1], Mobility Anchor Point [2]) which are either located in the Home or Visited Domain.

The mobile node may share a security association with its home AAA server for entity authentication to allow him to roam in different other domains. The idea described in this draft is that such security association can be used to create derivative security associations between the mobile node and other entities in the visited or home

domain. The keys thus established between the nodes can not only be used for authentication as required by Mobile IP and many of its extensions but additionally for confidentiality (e.g. over the access link between the mobile node and the access router) or other security services if required. This document specifies mechanisms and extensions to the Mobile IP to distribute security information to the mobile node.

1. Introduction

Mobile IP and many of its extensions such as Mobile IPv6 Regional Registration [1] or Hierarchical MIPv6 Mobility Management [2] require strong authentication between the mobile node and different agents (Home Agent, Gateway Mobility Agent [1], Mobility Anchor Point [2])which are either located in the Home or Visited Domain.

The mobile node may share a security association with its home AAA server for entity authentication to allow him to roam in different other domains: the idea is that when the mobile node enters a new visited domain, the serving system may want to authenticate the user to make sure he is a valid one before giving him access to its network resources, and the security association between the mobile node and the home domain is used to support such authentication.

The security association between the mobile node and the home domain security association can also be used to create derivative security associations between the mobile node and other entities in the visited or home domain (e.g. AAA in visited domain). The derivative security associations thus established between the nodes can not only be used for authentication as required by Mobile IP and many of its extensions but additionally used for confidentiality (e.g. over the access link between the mobile node and the access router) or other security services if required. This document specifies mechanisms and extensions to the Mobile IP to distribute security information to the mobile node.

Two methods are described in this document to support key distribution. The first method described is based on random numbers and the second one is based on the Diffie Hellman mechanism.

This document actually introduces the concept and future revisions will include more implementation details.

2. Definitions

Perfect forward Secrecy:

> A protocol is said to have perfect forward secrecy if compromise of long-term keys does not compromise past session keys.

3. Background and Motivation

Different key distribution schemes have already been introduced such as the ones described in "AAA Keys for Mobile IP" [3], or "Registration keys for Route Optimization" [4]. All such proposal suggest to distribute the key to the mobile node over the access link by encrypting it either using a long term security association between the mobile node and the AAA-H or using Public keys.

When considering radio links, sending the keys encrypted with a long term security association over the air interface causes a weak link in the security chain: the wireless link is weak since everyone can eavesdropp and the risk to have the long term key compromised is high. In fact, even if the keys are distributed by encrypting them, traditionally such key distribution mechanisms have been avoided in order to increase the system security. In addition, in such mechanism, once the long term key is compromised, the network can not distribute new keys to the MN.

For that reason, security keys in cellular networks (e.g. GSM, UMTS, IS-41) are never distributed over the air.

For the same reasons, in the present key distribution mechanisms used today such as Internet Key Exchange [5], keys are not distributed encrypted using a long term key: nonces, hash, Diffie Hellman values can be encrypted but the keys are not distributed, even encrypted.

Moreover, mechanisms proposed in [3], [4] do not provide Perfect Forward Secrecy.

As for the utilization of Public Keys as suggested in the current proposals, in addition to the high risk to have the Public Keys compromised by using them over the access link, and the lack of Perfect Forward Secrecy, in order for public keys solutions to be widely and efficiently deployed in commercial systems such as cellular networks, a well established PKI needs to exist. Moreover, many issues still need to be solved for the adoption of public keys in wireless networks: first of all, the limitated availability of the radio resources must be taken into account thus raising problems such as the procedure and the frequency for certificate revocation, and the certificate length itself. In addition, public keys based algorithms are also more time consuming, thus creating delay issues, and are more CPU demanding: low end mobile nodes may not be able to support the requirements of public key algorithms.

Diffie Hellman based key distribution is a viable alternative to establish the security associations between the mobile node and entities in the visited or home domains. Internet Key Exchange is

based on Diffie Hellman mechanism but IKE may not be appropriate for a wireless network: it requires too many messages to be exchanged over the access link and we need to consider that radio resources are a very limited and expensive resource.

Although IKE may not be the best solution for a cellular environment, a simpler and lighter key distribution based on Diffie Hellman will enable to re-apply the work of the IPsec Working Group to the Diffie Hellman mechanism. Furthermore key distribution based on Diffie Hellman can provide Perfect Forward Secrecy.

In summary, this document proposes to add two other key distribution mechanism to the mechanisms that already exist: a method based on random numbers and one based on the Diffie Hellman mechanism.

4. Key distribution based on random numbers

4.1. Background

In current cellular networks, key distribution is based on random

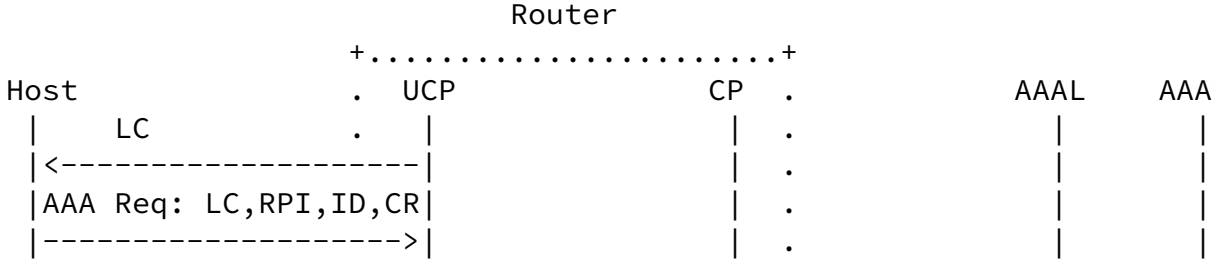
number. The Mobile Station and the Home Network share a long term key and have knowledge of a common authentication and key generation algorithm (e.g. CAVE in IS 41). Either the Home Network or the visited network generates the random number, depending on the specific cellular system considered. In the latter case, the visited domain informs the Home network of the value of the random number using inter domain security (e.g. thanks to a security association established through a roaming agreement).

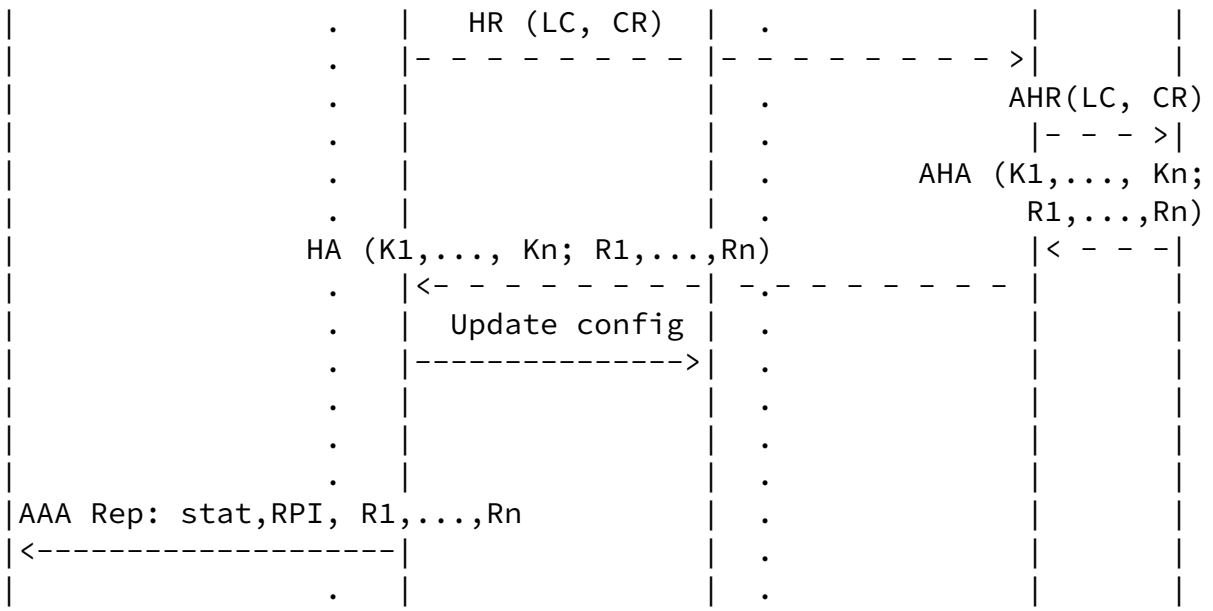
The random number is then sent to the Mobile station and using the long-term key and the common authentication and key generation algorithm, the MS derives the session keys. The Home Domain, having the same long-term key and authentication and key generation algorithms can also compute the same keys. It can then forwad them, protected using the inter domain security assocation, to the visited domain if the keys need to be shared between the mobile station and the visited domain.

In such a mechanism, over the access link, only the random number and the response to the authentication need to be sent. Even if they are eavesdropped this does not compromise the security since the eavesdropper does not know the long term key and cannot compute the session keys. This mechanism does not require to send the long term key over the access link, thus reducing the risk of having it compromised.

4.2. Basic procedure

In the AAA framework, the Local Challenge [6] broadcasted by the visited domain in Router advertisments messages can be used as the random number to derive the session keys. The following procedure describes how key distribution takes place.





LC = Local AAA Challenge
RPI = Replay Protection Indicator used between host and AAAH
CR = AAA Credential
ID = Client Identifier
UCP = Uncontrolled part
CP = Controlled part
AHR = AAA Host Request (using an AAA protocol)
AHA = AAA Host Answer (using an AAA protocol)
K1, ..., Kn = Session Keys
R1, ..., Rn = Random values

The Local challenge is then transmitted to the Home domain in the AHR message, protected using inter AAA servers security. Thanks to the

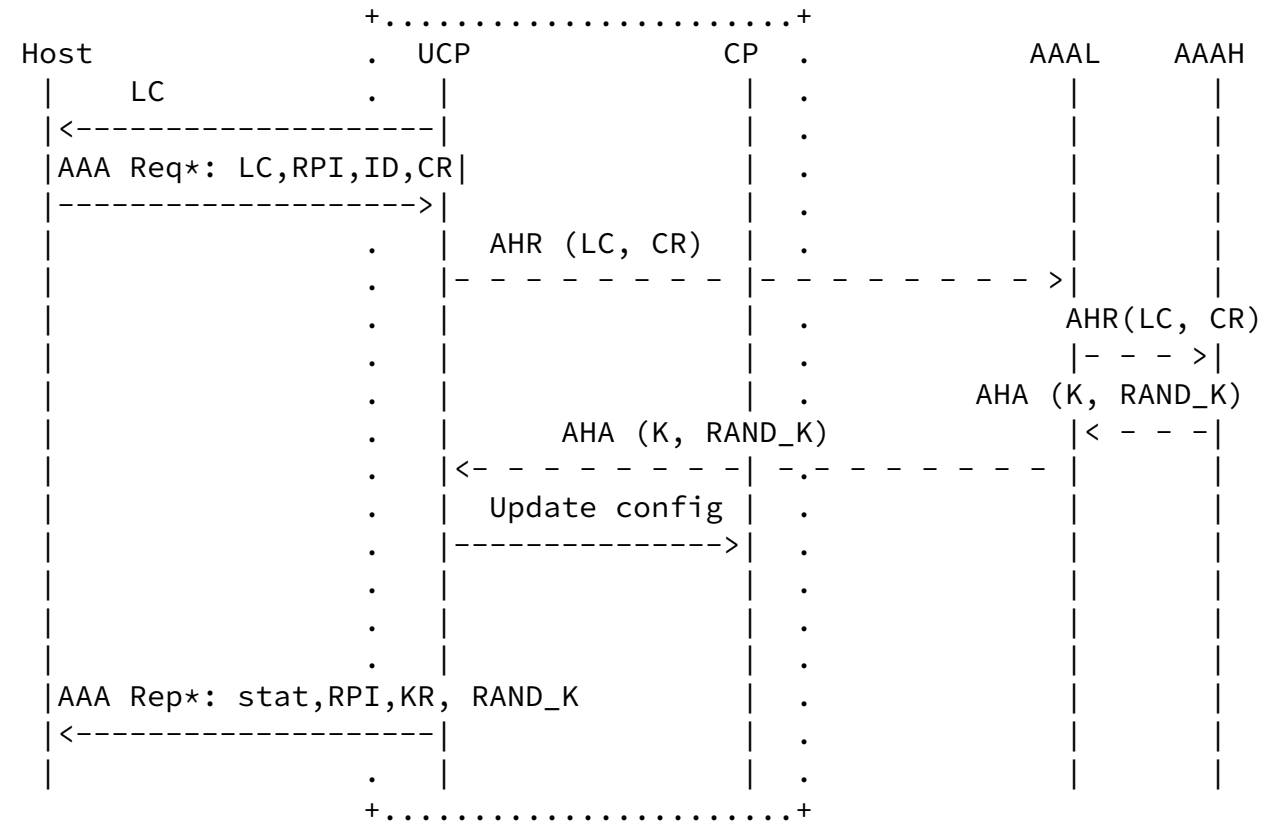
Client Identifier (e.g. the user's NAI) AAA-H retrieves the user specific long-term key and using the shared authentication and key generation algorithm, AAA-H derives the session keys K1-Kn.

The session keys are provided to the appropriate entities that will adopt them. Examples of session keys are the key used by the mobile node and the Home Agent for authenticating binding updates and Binding acknowledgement messages, and possible key shared by the

mobile node and mobility agents. If this agent is in the Home network, AAA-H forwards the value of the session keys using intra domain security. Otherwise, if the agent is in the visited domain, AAA-H transmits the session keys in a AHA message protected using inter AAA servers security, and the AAA-L forwards the session keys to the corresponding agents using visited domain intra domain security.

4.3. Enhanced procedure

In the previous case, the messages exchanged with the mobile node during the key distribution procedure are in clear text. The mechanism can be enhanced to provide confidentiality and authentication of the first messages as described in the follow:



Note: (*) indicates that the message is ciphered and integrity protected as described below.

The mobile node takes the Local Challenge and using the long term key and a key derivation algorithm it shares with its Home domain, it derives a Temporal Ciphering Key and an Temporal Integrity Key. The mobile node then creates the AAA Req message and encapsulates the Binding Update message; it also uses the previously computed keys to encrypt and integrity protect the message but leaving the Client Identifier in Clear text.

The Visited domain forwards this message to the AAA-H for user authentication, including the value of the Local Challenge.

The AAA-H retrieves the user specific long term key thanks to the Client ID, and using the Local Challenge, derives the Temporal Ciphering Key and Temporal Integrity Key to decrypt the message. AAA-H then verifies the authenticity of the user based on the AAA credentials and generates a random number RAND_K. Based on this value, using the user specific long term key and the common authentication and key generation algorithm it shares with the MN, it derives a key K.

AAA-H then forwards K to AAA-L using inter AAA servers security and uses the Temporal Ciphering Key and the Temporal Intergrity Key to secure the message to the MN carrying RAND_K. As indicated in the basic procedure, the AAA-H may distribute K to some entity, e.g. the Home Agent.

When receiving the reply, the MN uses the Temporal Ciphering Key and Temporal Integrity Key to decrypt the message and using RAND_K, derive the session key to be used.

The advantage of this mechanism is that it gives more control to the Home network since AAA-H generates the random number RAND_K used for the computation of the session keys and, in addition, provides more security since the messages exchanged with the mobile node during the key distribution procedure can be protected using the Temporal Ciphering Key and Temporal Intergrity Key. Finally RAND_K is also encrypted when sent to the MN.

5. Key distribution based on Diffie Hellman mechanism

5.1. Background

In the key distribution solutions proposed in the previous section, the AAA-H acts as a Key Distribution Center, generating the session keys and thus having knowledge of the keys used.

In a key distribution based on the Diffie Hellman mechanism, only the MN and the appropriate entities (i.e. the entities that will be using the keys for securing communications) have knowledge of the keys. Restricting the knowledge of the security key only to the entities that will actually use the keys is particularly useful in the following cases:

- when Home Agent is assigned in Visited Domain;
- for the security asociation to be used over the access link between the MN and the access router;
- for the security association to be set up between the MN and the mobility agents in the visited domain (when an extension such as [1] or [2] is deployed). In such cases the visited domain and the MN may not want the home domain to know the value of the session keys.

In addition, as mentioned above, the current proposals for Mobile IP key distribution does not provide Perfect Forward Secrecy whereas a

key distribution mechanism based on Diffie Hellman can provide that security service.

5.2. Diffie Hellman mechanism

As defined in [7], Diffie Hellman allows two nodes to derive a shared secret key for use in secret-key cryptography as follows:

Each node generates a random, secret value which it keeps private.

Each node computes a public value, derived mathematically from the random, secret value, and sends this public value to the other node.

Each node mathematically combines the public value received from the other node with its own random, secret value.

Due to the mathematical properties involved in the derivation of the public and secret values, the two nodes end up with the same exact combined values at the end of the procedure, which they can use as a shared secret key. In this exchange, the secret portions are not disclosed to anyone and therefore only these two nodes can compute the combined value.

Diffie-Hellman has a major vulnerability, though. Although it allows two nodes to establish a shared, secret key in a secure fashion, it does not allow a node to figure out with what other node it is establishing that specific secret key: an intruder on the path between two nodes could fool them into each establishing a key with the intruder instead of each other (man in the middle attack). To prevent this kind of man-in-the-middle attack and defeat such vulnerability, the Diffie Hellman Public value must be authenticated.

5.3. Procedure

As indicated above, in order to use the Diffie Hellman mechanism, the Diffie Hellman public values must be authenticated. In the Mobile IP/AAA framework, the security association between the Mobile node

and its home network (AAA-H) and the security association between the AAA-L and AAA-H can provide that authentication.

If the mobile node wants to set up a securiy association with an agent (e.g. home agent), the mobile node first sends its public Diffie Hellman value DH_MN using the long term security association it shares with its AAA-H to authenticate it. If the agent with whom the MN wants to set up a security association is in the visited domain, AAA-V retieves the agent's Diffie Hellman public value using

intra domain security and sends such value (authenticated with the security association it shares with the AAA-H) to the home network of the MN together with the message from the MN.

AAA-H authenticates the Diffie Hellman Public values of the agent and the MN, and then sends the MN's Diffie Hellman Public Value to the AAA-L using the security association it shares with AAA-L and encapsulates the Agent's Diffie Hellman Public Value to the MN using the security association it shares with the MN to authenticate it.

In this way, AAA-H is used to authenticate the Diffie Hellman public values but since it does not have knowledge of the secret values, it can not derive the secret. AAA-H is used as a certificate authority thus allowing an easy transition when Public Key Infrastructure will be deployed.

6. Possible optimizations thanks to the Temporary Shared Key

As described in [8], the Temporary Shared Key function encompasses the processes by which the authentication center (AAA-H) and the serving system (AAA-L) manage the sharing of authentication reponsibilities for a visiting MN.

Initially, the MN and its Home network (AAA-H) share a long term security association. When TSK is used, the Home network provides the serving system (AAA-L) with a user specific temporary Shared Key that that is shared between the serving system and the MN.

The temporary Shared Key refresh, set up and other related procedures are described in [8]. TSK Sharing gives the serving system

significant load control over the authentication and key distribution of a visiting MN: the key refresh and new key distribution procedure can be based on this temporary shared Key stored in the AAA-L thus saving round trips with the Home network.

Thanks to the TSK sharing function, the AAA-L can refresh and set up new keys for security associations between the MN and agents in the visited domain without involving the MN's home network.

This reduces time delay and load over the network.

This optimization can be applied both for the key distribution method based on random numbers and for the key distribution method based on the Diffie Hellman mechanism. In the first case, the serving system must have the common authentication and key generation algorithm and instead of using the long term key with the random number to compute

the session keys, the MN and the AAA-L use the temporary Shared Key and the random number as the inputs to the common authentication and key generation algorithm. In the second case, the MN uses the temporary Shared Key to authenticate its Diffie Hellman public value. The AAA-L does not need to invoke the AAA-H to verify the identity of the node sending the public value.

These are possible optimizations to the key distribution mechanisms but whether the TSK function is used depend on policies of the Home and Visited networks.

7. Security Considerations

The focus of this document is to provide the appropriate level of security for Mobile IP entities (mobile node,home agent, mobility agent) to operate Mobile IP Binding Update, binding acknowledgement. The security associations resulting from use of the suggested mechanisms can also offer other security services between the mobile node and entities in the visited domain.

8. Intellectual Property Considerations

Nokia Corporation and/or its affiliates hereby declare that they are in conformity with Section 10 of RFC 2026. Nokia's contributions may contain one or more patents or patent applications. To the extent Nokia's contribution is adopted to the specification, Nokia undertakes to license patents technically necessary to implement the specification on fair, reasonable and nondiscriminatory terms based on reciprocity.

9. References

[1] Jari T. Malinen and Charles E. Perkins. Mobile IPv6 Regional Registrations. Internet Draft, Internet Engineering Task Force, December 2000.

[2] Hesham Soliman, Claude Castelluccia, Karim El-Malki, and Ludovic Bellier. Hierarchical MIPv6 mobility management. Internet Draft, Internet Engineering Task Force, September, 2000.

[3] Charles E. Perkins and Pat R. Calhoun. AAA Registration Keys for Mobile IP. Internet Draft, Internet Engineering Task Force, January 2001.

[4] Charles E. Perkins, David B. Johnson, Carnegie Mellon University and N. Asokan. Registration Keys for Route Optimization. Internet Draft, Internet Engineering Task

Force, July 2000.

[5] D. Harkins and D. Carrel Internet Key Exchange. Request for Comments 2409, Internet Engineering Task Force, November 1998.

[6] N. Asokan, Patrik Flykt, Charles E. Perkins and Thomas Eklund AAA for IPv6 Network Access. Internet Draft, Internet Engineering Task Force, January 2000.

[7] Diffie, W. and Hellman, M., "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT-22, Nov. 1976, pp. 664- 654. IP [8] 10 Franck Le and Stefano M. Faccin. Temporary Shared Key Function for secure delegation of security to the local network. Internet Draft, Internet Engineering Task Force, February 2001.

10. Authors' Addresses

Franck Le
Nokia Research Center
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972 374-1256
E-mail: franck.le@nokia.com

stefano M. Faccin
Nokia Research Center
6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972 894-4994
E-mail: stefano.faccin@nokia.com

Table of Contents