Mobile IP Working Group
INTERNET DRAFT
28 January 2001

Charles E. Perkins
Nokia Research Center
Pat R. Calhoun
Sun Microsystems Laboratories

AAA Registration Keys for Mobile IP

draft-ietf-mobileip-aaa-key-03.txt

Status of This Memo

Abstract

AAA servers, such as RADIUS and DIAMETER, are in use within the Internet today to provide authentication and authorization services for dial-up computers. Mobile IP requires strong authentication between the mobile node and its home agent. When the mobile node shares a security association with its home AAA server, however, it is possible to use that security association to create derivative security associations between the mobile node and its home agent, and again between the mobile node and the foreign agent currently offering a care-of address to the mobile node. This document specifies extensions to the Mobile IP Registration Reply packet that can be used to distribute such security information to the mobile node.

1. Introduction

AAA servers, such as RADIUS [9] and DIAMETER [3], are in use within the Internet today to provide authentication and authorization services for dial-up computers. Such services are likely to be equally valuable for mobile nodes using Mobile IP when the nodes are attempting to connect to foreign domains with AAA servers. Mobile IP [7] requires strong authentication between the mobile node and its home agent. When the mobile node shares a security association with its home AAA server, however, it is possible to use that security association to create derivative security associations between the mobile node and its home agent, and again between the mobile node and the foreign agent currently offering a care-of address to the mobile node. This document specifies extensions to the Mobile IP Registration Reply packet that can be used to distribute such security information to the mobile node.

AAA servers typically use the Network Access Identifier (NAI) [1] to uniquely identify the mobile node; the mobile node's home address is not always necessary to provide that function. Thus, it is possible for a mobile node to authenticate itself, and be authorized for connection to the foreign domain, without even having a home address. However, for Mobile IP to work, the mobile node is required to have a security association with its home agent. When the Mobile IP Registration Reply packet is authenticated by the MN-AAA Authentication Extension [2], the mobile node can verify that the keys contained in the extensions were produced by the AAA server, and thus may be reliably used to create security associations with the home agent, or alternatively with the foreign agent.

The following operations are envisioned between the mobile node, AAA server, home agent, and foreign agent.

1. When a mobile node travels away from home, it may not have a security association with its home agent, perhaps because it does not yet have a home address.

2. When the mobile node first registers away from home, it includes a MN-AAA Authentication extension if it does not yet have a Mobility Security Association with a home agent.

3. At the time the information within the MN-AAA Authentication extension is verified by the AAA server, the AAA server also generates keys for the mobile node, encodes the keys according to its own security association with the mobile node, and causes insertion of the new key or keys along with the Registration Reply.

4. If the Reply passes authentication and contains the Unsolicited MN-HA Key From AAA extension (see section 6), the mobile node decodes the key according to its security association with the AAA. The resulting key is used to establish the mobile node's security association with its home agent, and is used to authenticate the MN-HA authentication extension.

5. Similarly, if the Reply passes authentication and contains the Unsolicited MN-FA Key From AAA extension (see section 4), the mobile node decodes the key according to its security association with the AAA. The resulting key is used to establish the mobile node's security association with its new foreign agent, and is used to compute the authentication data used in the MN-FA authentication extension.

Any registration reply containing the Unsolicited MN-HA Key From AAA extension MUST also contain a subsequent Mobile Home Authentication Extension, created using the decrypted version of the MN-HA key. Similarly, a reply containing the Unsolicited MN-FA Key From AAA extension MUST also contain a subsequent Mobile Foreign Authentication Extension, created using the decrypted version of the MN-FA key.

2. Security Algorithms

Mobility Security Associations between Mobile IP entities (mobile nodes, home agents, foreign agents) contain both the necessary cryptographic key information, and a way to identify the cryptographic algorithm which uses the key to produce the authentication information typically included in the Mobile Home Authentication extension or the Mobile Foreign Authentication extension. In order for the mobile node to make use of key information sent to it by the AAA server, the mobile node also has to be able to select the appropriate cryptographic algorithm that uses the key to produce the authentication.

For use with the key extensions specified in this document, the supported security algorithms are also specified. In order for a mobile node to be able to decode the keys defined in this document, it MUST share a security association with its' Home AAA server. The security association is the one by which the mobile node is instructed to decode the keying material in the the Unsolicited MN-FA or MN-HA Key From AAA extensions.

Reserved SPI number	Name	Reference
3	MD5/prefix+suffix	RFC 2002 [7]

New algorithms will be allocated as indicated by practical experience using the extensions defined in this document. See section 3 for specific information about using Algorithm MD5/prefix+suffix. The HMAC MD5 algorithm is used in exactly the same way, except that the specific computation used with MD5 follows RFC 2104 instead of RFC 2002.

3. Using the MD5/prefix+suffix Algorithm

As with Mobile IP, all mobile nodes MUST be able to verify the authenticator within a MN-HA Authentication extension by using MD5 in prefix+suffix mode, signified by selection at a SPI of any arbitrary 32-bit value. Therefore, it is economical to use the MD5 algorithm in prefix+suffix mode to encode the key within the particular key extension, as follows.

1. The AAA server identifies the mobile node's IP address, call it ``node-address''.

2. The AAA server calculates

   (key XOR (MD5(AAA-key | node-address | AAA-key)))

3. The AAA server inserts this result into the Key extension in the ``Encoded Key'' field.

4. The mobile node calculates

   temp = MD5(AAA-key | node-address | AAA-key)

5. The mobile node extracts the Security_Information of the key extension and calculates

   key = Encoded Key XOR temp

4. Unsolicited MN-FA Key From AAA Subtype

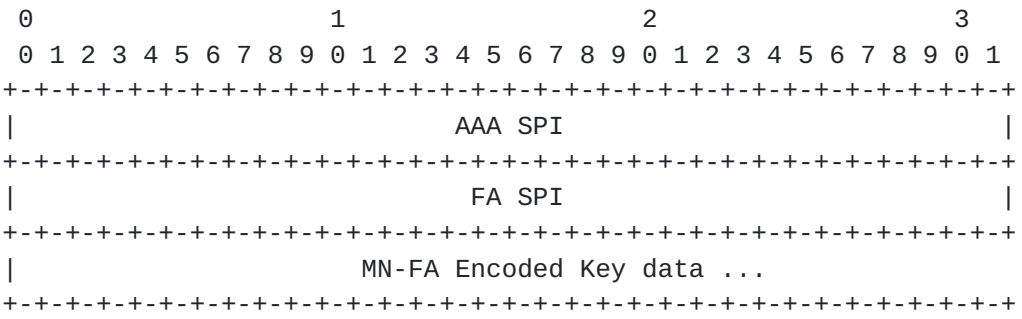

Figure 1: The Unsolicited MN-FA Key From AAA Subtype-Specific Data

AAA SPI A 32-bit opaque value, indicating the SPI that the mobile node must use to determine the algorithm to use for recovering the FA security information.

FA SPI A 32-bit opaque value, which the mobile node MUST use to index all the necessary information recovered from the FA security information after it is decoded.

MN-FA Encoded Key data
The necessary information (including the key) required by the mobile node to create a Mobility Security Association between itself and the foreign agent.

The Unsolicited MN-FA Key From AAA extension, shown in figure 1, uses subtype 7 of the Generalized MN-FA Key Reply Extension [8]. The key is encoded by the home domain AAA server (AAAH) for use by the mobile node to secure future Mobile IP registrations with the same foreign agent. The Unsolicited MN-FA Key From AAA extension MUST appear in the Registration Reply before the MN-FA Authentication extension.

Once the mobile node decodes the FA Security Information, by using the algorithm indexed by the AAA SPI, it stores the FA Security Information indexed by the FA SPI in its list of Mobile Security Associations.

If the foreign agent receives a Registration Reply that does not have a Unsolicited MN-FA Key From AAA extension, and thus does not have a way to establish a Mobility Security Association with the mobile node, the foreign agent SHOULD change the Code value of the Registration Reply to MISSING_MN_FA (see section 7), effectively causing the registration to fail.

5. Generalized MN-HA Key Reply Extension

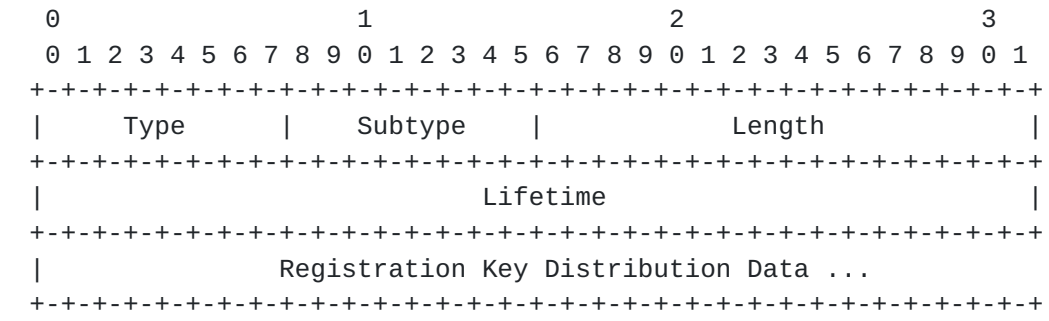

Figure 2: The Generalized Mobile IP MN-HA Key Reply Extension

Type — 42 (not skippable) (see [7])

Subtype — a number assigned to identify the way in which the Encoded Registration Key Data is to be decrypted to obtain the registration key

Length — The 16-bit Length field indicates the length of the extension. It is equal to 4 plus the number of bytes in the Encoded Registration Key Data.

Lifetime — This field indicates the duration of time (in seconds) for which the MH-HA key is valid.

Registration Key Distribution Data — An encrypted copy of the registration key, along with any other information needed by the mobile node to create the designated Mobility Security Association with the home agent.

6. Unsolicited MN-HA Key From AAA Subtype

The Unsolicited MN-HA Key From AAA is subtype 1 of the Generalized MN-HA Key Reply Extension (see section 5).

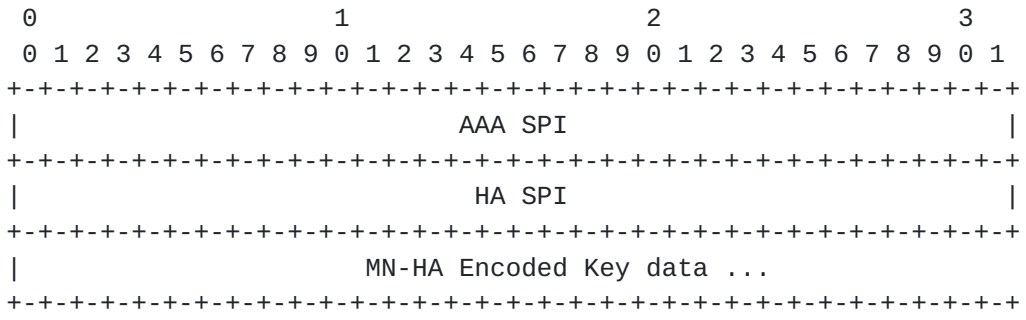

Figure 3: The Unsolicited MN-HA Key From AAA Subtype-Specific Data

AAA SPI A 32-bit opaque value, indicating the SPI that the mobile node must use to determine the algorithm to use for recovering the HA security information.

HA SPI A 32-bit opaque value, which the mobile node MUST use to index all the necessary information recovered from the HA security information after it is decoded.

MN-HA Encoded Key data
The necessary information (including the key) required by the mobile node to create a Mobility Security Association between itself and the home agent.

The Unsolicited MN-HA Key From AAA subtype-specific data is shown in figure 3. The Mobile Node Encoded Key data is to be decoded according to the given SPI between the mobile node and the home domain AAA server (AAAH). The key is intended for use the mobile node to secure future Mobile IP registrations with its home agent. The MN-HA Key Reply MUST appear in the Registration Reply before the MN-HA Authentication extension.

Once the mobile node decodes the MN-HA Encoded Key data, by using the algorithm indexed by the AAA SPI, it stores the HA Security Information indexed by the HA SPI in its list of Mobile Security Associations. The mobile node uses the Identification field data from the Registration Request as its initial synchronization data with the home agent.

7. Error Values

Each entry in the following table contains the name of Code [7] to be returned in a Registration Reply, the value for the Code, and the section in which the error is first mentioned in this specification.

Error Name	Value	Section
MISSING_MN_FA	107	4

8. IANA Considerations

The number for the Generalized MN-HA Key Reply Extension is taken from the numbering space defined for Mobile IP registration extensions defined in RFC 2002 [7] as extended in RFC 2356 [6].

The subtype address space for the Generalized MN-HA Key Reply extension is defined in this document. From this space, subtype value 1 is assigned to the Unsolicited MN-HA Key From AAA Subtype extension.

The number assigned to the Unsolicited MN-FA Key From AAA Subtype extension was taken from the numbering space defined for the Generalized MN-FA Key Reply Extension, defined in [8].

The Code values specified for errors, listed in section 7, MUST NOT conflict with any other code values listed in RFC 2002, RFC 2344 [5], or RFC 2356 [6]. They are to be taken from the space of error values conventionally associated with rejection by the foreign agent (i.e., 64-127).

SPI values 3 and 4 are taken from the reserved space of SPI numbers (0-255) created for special Mobile IP algorithm identifiers.

9. Security Considerations

The extensions in this document are intended to provide the appropriate level of security for Mobile IP entities (mobile node, foreign agent, and home agent) to operate Mobile IP registration protocol. The security associations resulting from use of these extensions do not offer any higher level of security than what is already implicit in use of the security association between the mobile node and the AAA.

References

[1] B. Aboba and M. Beadles. The Network Access Identifier. Request for Comments (Proposed Standard) 2486, Internet Engineering Task Force, January 1999.

[2] P. Calhoun and C. E. Perkins. Mobile IP Foreign Agent Challenge/Response Extension. draft-ietf-mobileip-challenge-08.txt, January 2000. (work in progress).

[3] P. Calhoun, A. Rubens, H. Akhtar, and E. Guttman. DIAMETER Base Protocol. Internet Draft, Internet Engineering Task Force. draft-calhoun-diameter-12.txt, December 1999. Work in progress.

[4] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. Request for Comments (Informational) 2104, Internet Engineering Task Force, February 1997.

[5] G. Montenegro. Reverse Tunneling for Mobile IP. Request for Comments (Proposed Standard) 2344, Internet Engineering Task Force, May 1998.

[6] G. Montenegro and V. Gupta. Sun's SKIP Firewall Traversal for Mobile IP. Request for Comments (Informational) 2356, Internet Engineering Task Force, June 1998.

[7] C. Perkins. IP Mobility Support. Request for Comments (Proposed Standard) 2002, Internet Engineering Task Force, October 1996.

[8] C. Perkins and D. Johnson. Registration Keys for Route Optimization. Internet Draft, Internet Engineering Task Force, December 1997. Work in progress.

[9] C. Rigney, A. Rubens, W. Simpson, and S. Willens. Remote Authentication Dial In User Service (RADIUS). Request for Comments (Proposed Standard) 2138, Internet Engineering Task Force, April 1997.

Addresses

The working group can be contacted via the current chairs:

Basavaraj Patil
Nortel Networks Inc.
2201 Lakeside Blvd.
Richardson, TX. 75082-4399
USA
Phone: +1 972-684-1489
EMail: bpatil@nortelnetworks.com

Phil Roberts
Motorola
1501 West Shure Drive
Arlington Heights, IL 60004
USA
Phone: +1 847-632-3148
EMail: QA3445@email.mot.com

Questions about this memo can also be directed to the authors:

Charles E. Perkins
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1-650 625-2986
EMail: charliep@iprg.nokia.com
Fax: +1 650 625-2502

Pat R. Calhoun
Network & Security Center
Sun Microsystems Laboratories
15 Network Circle
Menlo Park, California 94025
USA
Phone: +1 650-786-7733
EMail: pcalhoun@eng.sun.com
Fax: +1 650-786-6445