Mobile IP Working Group   Charles E. Perkins
INTERNET DRAFT   Nokia Research Center
20 July 2001   Pat R. Calhoun
                                               Sun Microsystems Laboratories

AAA Registration Keys for Mobile IP

draft-ietf-mobileip-aaa-key-08.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 connectivity to the mobile node. This document specifies extensions to the Mobile IP Registration Reply packet that can be used to create such security information at the mobile node.

1. Introduction

AAA servers, such as RADIUS [13] and DIAMETER [4], 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 [11] 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 connectivity to the mobile node. This document specifies extensions to the Mobile IP Registration messages that can be used to create those security associations at 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 having any 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 [3], 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 key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [2].

2. Scope of Protocol

The protocol and messages in this document are intended to facilitate the following operations which may occur 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. If the mobile node does not have a Mobility Security Association with the foreign agent, it SHOULD include an MN-FA Key Request extension.

3. Similarly, if the mobile node does not have a Mobility Security Association with the home agent, it MUST add an MN-HA Key Request extension.

4. If one or more Key Request extensions were added, the MN-AAA Authentication extension is added to the Registration Request.

5. At the time the information within the MN-AAA Authentication extension is verified by the AAA server, the AAA server also generates Key Material for the keys requested by the mobile node, and causes insertion of the Key Material fields along with the Registration Reply.

6. The respective AAA keys are distributed to the Home and Foreign Agent via the AAA protocol.

7. If the Reply passes authentication and contains the Unsolicited MN-HA Key Material From AAA extension (see section 6), the mobile node generates the key using the Key Material provided, 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.

8. Similarly, if the Reply passes authentication and contains the Unsolicited MN-FA Key Material From AAA extension (see section 5), the mobile node generates the key using the Key Material provided, 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 Material From AAA extension MUST also contain a subsequent Mobile Home Authentication Extension, created using the generated MN-HA key. Similarly, a reply containing the Unsolicited MN-FA Key Material From AAA extension MUST also contain a subsequent Mobile Foreign Authentication Extension, created using the the MN-FA key.

3. Dynamic Security Associations

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. The following table contains the supported algorithm identifiers.

Algorithm Identifier	Name	Reference
1	MD5/prefix+suffix	RFC 2002 [11]
2	HMAC MD5	RFC 2104 [6]
3	SHA-1	FIPS 180-1 [10]

New algorithms will be allocated as indicated by practical experience using the extensions defined in this document.

Dynamic Mobility Security Associations shared between mobile nodes and home agents also requires a replay protection method. The following table contains the supported replay methods.

Replay Method	Name	Reference
1	None	RFC 2002 [11]
2	Timestamps	RFC 2002 [11]
3	Nonces	RFC 2002 [11]

4. Key Material Creation and Derivation

This section contains the procedures followed in the creation of the Key Material by AAA servers, and the key derivation procedures used by mobile nodes. Note that the AAA servers will also make use of the derivation procedures to deliver the keys via the AAA protocol.

The example that follows makes use of MD5 in prefix+suffix mode, whose support is mandatory in Mobile IP [11]. Other cryptographic functions, such as those listed in 3 MAY also be used.

1. The AAA server identifies the mobile node's via a ``node-address''. If the Home Address field of the Registration Request is zero (0), the Mobile Node's NAI is used instead.

2. The AAA server generates a random [5] value of at least 64 bits.

3. The AAA server inserts the random value into the Key extension in the ``Key Material'' field.

4. The mobile node calculates

   key = MD5(AAA-key | Key Material | node-address | AAA-key)

5. The mobile node creates the dynamic security association, using the key, and the other relevant information in the Key Extension.

5. Unsolicited MN-FA Key Material From AAA Subtype

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Lifetime                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            AAA SPI                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             FA SPI                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Algorithm Identifier     |      Key Material ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

lifetime   This field indicates the duration of time (in seconds) for which the MN-FA key is valid.

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

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

Algorithm Identifier
This field indicates the algorithm to be used for future computations of the MN-FA Authentication Extension (see section 3)

Key Material
A random [5] value of at least 64 bits.

The Unsolicited MN-FA Key Material From AAA extension, shown in figure 1, uses subtype 7 of the Generalized MN-FA Key Reply

Extension [12]. The Key Material is added by the home domain AAA server (AAAH) for use by the mobile node in creating the MN-FA key, which is used to secure future Mobile IP registrations with the same foreign agent. The Unsolicited MN-FA Key Material From AAA extension MUST appear in the Registration Reply before the MN-FA Authentication extension.

Once the mobile node creates 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 has no Unsolicited MN-FA Key Material From AAA extension, and thus cannot establish a Mobility Security Association with the mobile node, the foreign agent MAY change the Code value of the Registration Reply to MISSING_MN_FA (see section 9), effectively causing the registration to fail.

6. Unsolicited MN-HA Key Material From AAA Subtype

The Unsolicited MN-HA Key Material From AAA is subtype 1 of the Generalized MN-HA Key Reply Extension [12].

```
       0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                            AAA SPI                            |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                             HA SPI                            |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |     Algorithm Identifier      |         Replay Method         |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                         Key Material ...
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: The Unsolicited MN-HA Key Material 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 establishing the HA security information.

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

Algorithm Identifier
This field indicates the algorithm to be used for future computations of the MN-HA Authentication Extension (see section 3)

Replay Method
This field contains the replay method to be used for future Registration messages (see section 3).

Key Material
A random [5] value of at least 64 bits.

The Unsolicited MN-HA Material Key From AAA subtype-specific data is shown in figure 2. The Mobile Node creates the MN-HA key using the Key Material provided by 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 creates the MN-HA Key, by using the algorithm specified in 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. MN-FA Key Request From AAA Subtype

The MN-FA Key Request From AAA subtype data uses subtype 7 of the Generalized MN-FA Key Request Extension [12]. The MN-FA Key Request From AAA extension MUST appear in the Registration Request before the MN-AAA Authentication extension. The subtype data field is zero in length.

8. MN-HA Key Request From AAA Subtype

The MN-HA Key Request From AAA subtype data uses subtype 7 of the Generalized MN-HA Key Request Extension [12]. The MN-HA Key Request From AAA extension MUST appear in the Registration Request before the

MN-AAA Authentication extension. The subtype data field is zero in length.

9. Error Values

Each entry in the following table contains the name of Code [11] 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	5

10. 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 [11] as extended in RFC 2356 [8].

The number 7, assigned to the Unsolicited MN-HA Key Material From AAA Subtype extension, was taken from the numbering space defined for the Generalized MN-HA Key Reply Extension, defined in [12].

The number 7, assigned to the MN-FA Key Request From AAA Subtype extension, was taken from the numbering space defined for the Generalized MN-FA Key Request Extension, defined in [12].

The number 1, assigned to the Unsolicited MN-FA Key Material From AAA Subtype extension, was taken from the numbering space defined for the Generalized MN-FA Key Reply Extension, defined in [12].

The number 7, assigned to the MN-HA Key Request From AAA Subtype extension, was taken from the numbering space defined for the Generalized MN-HA Key Request Extension, defined in [12].

The Code values specified for errors, listed in section 9, MUST NOT conflict with any other code values listed in RFC 2002, RFC 3024 [7], or RFC 2356 [8]. They are to be taken from the space of error values conventionally associated with rejection by the foreign agent (i.e., 64-127).

Section 3 introduces the Algorithm Identifier namespace that requires IANA management. This specification makes use of 1-3; all other values other than zero (0) are available for assignment, pending review and approval by a Designated Expert [9].

Section 3 introduces the Replay Method Identifier namespace that requires IANA management. This specification makes use of 1-3; all other values other than zero (0) are available for assignment, pending review and approval by a Designated Expert [9].

11. 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.

Since the extensions defined in this specification only carries Key Material, which is used to derive keys, it does not expose any data that could be used in an attack aimed at recovering the key shared between the mobile node and the AAA. The authors do not believe this specification introduces new security risks.

References

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

[2] S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. Request for Comments (Best Current Practice) 2119, Internet Engineering Task Force, March 1997.

[3] P. Calhoun and C. E. Perkins. Mobile IP Foreign Agent Challenge/Response Extension. Request for Comments (Proposed Standard) 3012, Internet Engineering Task Force, December 2000.

[4] P. Calhoun, A. Rubens, H. Akhtar, and E. Guttman. DIAMETER Base Protocol (work in progress). Internet Draft, Internet Engineering Task Force. draft-ietf-aaa-diameter-07.txt, July 2001.

[5] D. Eastlake, 3rd, S. Crocker, and J. Schiller. Randomness Recommendations for Security. Request for Comments (Informational) 1750, Internet Engineering Task Force, December 1994.

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

[7] Editor G. Montenegro. Reverse Tunneling for Mobile IP, revised. Request for Comments (Proposed Standard) 3024, Internet Engineering Task Force, January 2001.

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

[9] T. Narten and H. Alvestrand. Guidelines for Writing an IANA Considerations Section in RFCs. Request for Comments (Best Current Practice) 2434, Internet Engineering Task Force, October 1998.

[10] National Institute of Standards and Technology. Secure Hash Standard. Technical Report NIST FIPS PUB 180-1, U.S. Department of Commerce, April 1995.

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

[12] C. Perkins and P. Calhoun. Generalized Key Distribution Extensions for Mobile IP (work in progress). draft-ietf-mobileip-gen-key-01.txt, July 2001.

[13] C. Rigney, A. Rubens, W. Simpson, and S. Willens. Remote Authentication Dial In User Service (RADIUS). Request for Comments (Proposed Standard) 2865, Internet Engineering Task Force, June 2000.

Addresses

The working group can be contacted via the current chairs:

Basavaraj Patil
Nokia
6000 Connection Dr.

Irving, TX. 75039
USA
Phone: +1 972-894-6709
Email: Basavaraj.Patil@nokia.com

Phil Roberts
Megisto Corp.
Suite 120
20251 Century Blvd
Germantown MD 20874
USA
Phone: +1 847-202-9314
Email: PRoberts@MEGISTO.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