Network Working Group
Internet-Draft
Expires: August 3, 2006

Charles E. Perkins
Nokia Research Center
Pat R. Calhoun
Cisco Systems, Inc.
Jayshree. Bharatia
Nortel Networks
January 30, 2006

Mobile IPv4 Challenge/Response Extensions (revised)
draft-ietf-mip4-rfc3012bis-05.txt

Status of this Memo

Copyright Notice

Abstract

Mobile IP, as originally specified, defines an authentication extension (the Mobile-Foreign Authentication extension) by which a mobile node can authenticate itself to a foreign agent. Unfortunately, that extension does not provide the foreign agent any direct guarantee that the protocol is protected from replays, and

does not allow for the use of existing techniques (such as CHAP) for authenticating portable computer devices.

In this specification, we define extensions for the Mobile IP Agent Advertisements and the Registration Request that allow a foreign agent to use a challenge/response mechanism to authenticate the mobile node.

Furthermore, this document updates RFC3344 by including new authentication extension called the Mobile-AAA Authentication extension. This new extension is provided so that a mobile node can supply credentials for authorization using commonly available AAA infrastructure elements. This Authorization-enabling extension MAY co-exist in the same Registration Request with Authentication extensions defined for Mobile IP Registration by RFC3344. This document obsoletes RFC3012.

Table of Contents

1. Introduction 4
1.1. Terminology 4
2. Mobile IP Agent Advertisement Challenge Extension 6
2.1. Handling of Solicited Agent Advertisements 6
3. Operation 8
3.1. Mobile Node Processing of Registration Requests 8
3.2. Foreign Agent Processing of Registration Requests 9
3.2.1. Foreign Agent Algorithm for Tracking Used Challenges 11
3.3. Foreign Agent Processing of Registration Replies 11
3.4. Home Agent Processing of Challenge Extensions 13
3.5. Mobile Node Processing of Registration Replies 13
4. Mobile-Foreign Challenge Extension 14
5. Generalized Mobile IP Authentication Extension 15
6. Mobile-AAA Authentication subtype 17
7. Reserved SPIs for Mobile IP 18
8. SPIs for RADIUS AAA Servers 19
9. Configurable Parameters 20
10. Error Values 21
11. IANA Considerations 22
12. Security Considerations 23
13. Acknowledgments 24
14. Normative References 24
Appendix A. Change History 25
Appendix B. Verification Infrastructure 26
Appendix C. Message Flow for FA Challenge Messaging with Mobile-AAA Extension 28
Appendix D. Message Flow for FA Challenge Messaging with MN-FA Authentication 30
Appendix E. Example Pseudo-Code for Tracking Used Challenges . . 31
Authors' Addresses 32
Intellectual Property and Copyright Statements 33

1. Introduction

Mobile IP defines the Mobile-Foreign Authentication extension to allow a mobile node to authenticate itself to a foreign agent. Such authentication mechanisms are mostly external to the principal operation of Mobile IP, since the foreign agent can easily route packets to and from a mobile node whether or not the mobile node is reporting a legitimately owned home address to the foreign agent. Unfortunately, that extension does not provide the foreign agent any direct guarantee that the protocol is protected from replays, and does not allow for the use of CHAP [RFC1994] for authenticating portable computer devices. In this specification, we define extensions for the Mobile IP Agent Advertisements and the Registration Request that allow a foreign agent to use challenge/ response mechanism to authenticate the mobile node. Furthermore, an additional authentication extension, the Mobile-AAA authentication extension, is provided so that a mobile node can supply credentials for authorization using commonly available AAA infrastructure elements. The foreign agent may be able to interact with an AAA infrastructure (using protocols outside the scope of this document) to obtain a secure indication that the mobile node is authorized to use the local network resources.

1.1. Terminology

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 RFC 2119 [RFC2119].

This document uses the term Security Parameters Index (SPI) as defined in the base Mobile IP protocol specification [RFC3344]. All SPI values defined in this document refer to values for the SPI as defined in that specification.

The following additional terminology is used in addition to that defined in [RFC3344]:

previously used challenge:

The challenge is a previously used challenge if the mobile node sent the same challenge to the foreign agent in a previous Registration Request, and that previous Registration Request passed all validity checks performed by the foreign agent. The foreign agent may not be able to keep records for all previously used challenges, but see Section 3.2 for minimal requirements.

security association:

A "mobility security association", as defined in [RFC3344].

unknown challenge:

Any challenge from a particular mobile node that the foreign agent has no record of having put either into one of its recent Agent Advertisements or into a registration reply message to that mobile node.

unused challenge:

A challenge that has not been already accepted by the foreign agent from the mobile node in the Registration Request -- i.e., a challenge that is neither unknown nor previously used.

2. Mobile IP Agent Advertisement Challenge Extension

This section defines a new extension to the Router Discovery Protocol [RFC1256] for use by foreign agents that need to issue a challenge for authenticating mobile nodes.

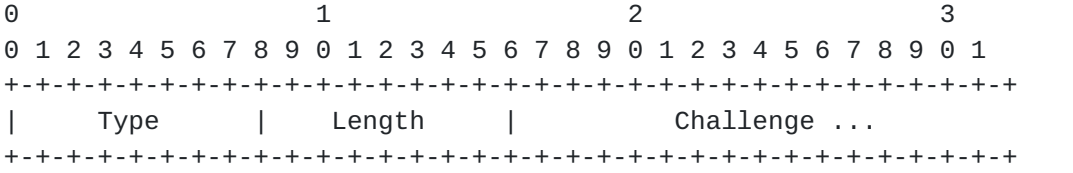

Figure 1: The Challenge Extension

Type:

24

Length:

The length of the Challenge value in bytes; SHOULD be at least 4

Challenge:

A random value that SHOULD be at least 32 bits

The Challenge extension, illustrated in Figure 1, is inserted in the Agent Advertisements by the foreign agent, in order to communicate a previously unused challenge value that can be used by the mobile node to compute an authentication for its next registration request message. The challenge is selected by the foreign agent to provide local assurance that the mobile node is not replaying any earlier registration request. Eastlake, et al. [RFC1750] provides more information on generating pseudo-random numbers suitable for use as values for the challenge.

Note that the storage of different Challenges received in Agent Advertisements from multiple foreign agents is implementation specific and hence, out of scope for this specification.

2.1. Handling of Solicited Agent Advertisements

When a foreign agent generates an Agent Advertisement in response to a Router Solicitation [RFC1256], some additional considerations come into play. According to the Mobile IP base specification [RFC3344], the resulting Agent Advertisement may be either multicast or unicast.

If the solicited Agent Advertisement is multicast, it MUST NOT generate a new Challenge value and update its window of remembered advertised Challenges. It must instead re-use the most recent of the CHALLENGE_WINDOW Advertisement Challenge values (Section 9).

If the agent advertisement is unicast back to the soliciting mobile node, it MUST be handled as follows: If the challenge most recently unicast to the soliciting mobile node has not been previously used (as defined in Section 1.1), it SHOULD be repeated in the newly issued unicast agent advertisement, otherwise a new challenge MUST be generated and remembered as the most recent challenge issued to the mobile node. For further discussion of this, see Section 12.

3. Operation

This section describes modifications to the Mobile IP registration process [RFC3344] which may occur after the foreign agent issues a Mobile IP Agent Advertisement containing the Challenge on its local link. See Appendix C for a diagram showing the canonical message flow for messages related to the processing of the foreign agent challenge values.

3.1. Mobile Node Processing of Registration Requests

Retransmission behavior for Registration Requests is identical to that specified in Mobile IP specification [RFC3344]. A retransmitted Registration Request MAY use the same Challenge value as given in the original Registration Request.

Whenever the Agent Advertisement contains the Challenge extension, if the mobile node does not have a security association with the foreign agent, then it MUST include the Challenge value in a Mobile-Foreign Challenge extension to the Registration Request message. If, on the other hand, the mobile node does have a security association with the foreign agent, it SHOULD include the Challenge value in its Registration Request message.

If the mobile node has a security association with the Foreign Agent, it MUST include a Mobile-Foreign Authentication extension in its Registration Request message, according to the base Mobile IP specification [RFC3344]. When the Registration Request contains the Mobile-Foreign Challenge extension specified in Section 4, the Mobile-Foreign Authentication MUST follow the Challenge extension in the Registration Request. The mobile node MAY also include the Mobile-AAA Authentication extension. If both the Mobile-Foreign Authentication and the Mobile-AAA Authentication extensions are present, the Mobile-Foreign Challenge extension MUST precede the Mobile-AAA Authentication extension and the Mobile-AAA Authentication extension MUST precede the Mobile-Foreign Authentication extension.

If the mobile node does not have a security association with the foreign agent, the mobile node MUST include the Mobile-AAA Authentication extension as defined in Section 6 when it includes the Mobile-Foreign Challenge extension. In addition, the mobile node SHOULD include the NAI extension [RFC2794], to enable the foreign agent to make use of available verification infrastructure which requires this. The SPI field of the Mobile-AAA Authentication extension specifies the particular secret and algorithm (shared between the mobile node and the verification infrastructure) that must be used to perform the authentication. If the SPI value is chosen as CHAP_SPI (see Section 9), then the mobile node specifies

CHAP-style authentication [RFC1994] using MD5 [RFC1321].

In either case, the Mobile-Foreign Challenge extension followed by one of the above specified authentication extensions MUST follow the Mobile-Home Authentication extension, if present.

A mobile node MAY include the Mobile-AAA Authentication extension in the Registration Request when the mobile node registers directly with its home agent (using a co-located care-of address). In this case, the mobile node uses an SPI value of CHAP_SPI (Section 8) in the MN-AAA Authentication extension and MUST NOT include the Mobile-Foreign Challenge extension. Also, replay protection for the Registration Request in this case is provided by the Identification field defined by [RFC3344].

3.2. Foreign Agent Processing of Registration Requests

Upon receipt of the Registration Request, if the foreign agent has issued a Challenge as part of its Agent Advertisements, and if it does not have a security association with the mobile node, then the foreign agent SHOULD check that the Mobile-Foreign Challenge extension exists, and that it contains a challenge value previously unused by the mobile node. This ensures that the mobile node is not attempting to replay a previous advertisement and authentication. In this case, if the Registration Request does not include a Challenge extension, the foreign agent MUST send a Registration Reply with the Code field set to set to MISSING_CHALLENGE.

If a mobile node retransmits a Registration Request with the same Challenge extension, and the foreign agent still has a pending Registration Request record in effect for the mobile node, then the foreign agent forwards the Registration Request to the Home Agent again. The foreign agent SHOULD check that the mobile node is actually performing a retransmission, by verifying that the relevant fields of the retransmitted request (including, if present, the mobile node NAI Extension [RFC2794]) are the same as represented in the visitor list entry for the pending Registration Request (section 3.7.1 of [RFC3344]). This verification MUST NOT include the "remaining Lifetime of the pending registration", or the Identification field since those values are likely to change even for requests that are merely retransmissions and not new Registration Requests. In all other circumstances, if the foreign agent receives a Registration Request with a Challenge extension containing a Challenge value previously used by that mobile node, the foreign agent SHOULD send a Registration Reply to the mobile node containing the Code value STALE_CHALLENGE.

The foreign agent MUST NOT accept any Challenge in the Registration

Request unless it was offered in the last Registration Reply or unicast Agent Advertisement sent to the mobile node, or else advertised as one of the last CHALLENGE_WINDOW (see Section 9) Challenge values inserted into the immediately preceding Agent advertisements. If the Challenge is not one of the recently advertised values, the foreign Agent SHOULD send a Registration Reply with Code value UNKNOWN_CHALLENGE (see Section 10). The foreign agent MUST maintain the last challenge used by each mobile node that has registered using any one of the last CHALLENGE_WINDOW challenge values. This last challenge value can be stored as part of the mobile node's registration records. Also, see Section 3.2.1 for a possible algorithm that can be used to satisfy this requirement.

Furthermore, the foreign agent MUST check that there is either a Mobile-Foreign, or a Mobile-AAA Authentication extension after the Challenge extension. Any registration message containing the Challenge extension without either of these authentication extensions MUST be silently discarded. If the registration message contains a Mobile-Foreign Authentication extension with an incorrect authenticator that fails verification, the foreign agent MAY send a Registration Reply to the mobile node with Code value BAD_AUTHENTICATION (see Section 10).

If the Mobile-AAA Authentication extension (see Section 6) is present in the message, or if an NAI extension is included indicating that the mobile node belongs to a different administrative domain, the foreign agent may take actions outside the scope of this protocol specification to carry out the authentication of the mobile node. If the registration message contains a Mobile-AAA Authentication extension with an incorrect authenticator that fails verification, the foreign agent MAY send a Registration Reply to the mobile node with Code value FA_BAD_AAA_AUTH. If the Mobile-AAA Authentication Extension is present in the Registration Request, the foreign agent MUST NOT remove the Mobile-AAA Authentication Extension and the Mobile-Foreign Challenge extension from the Registration Request, before forwarding to the home agent. Appendix C provides an example of an action that could be taken by a foreign agent.

In the event that the Challenge extension is authenticated through the Mobile-Foreign Authentication extension and the Mobile-AAA Authentication extension is not present, the foreign agent MAY remove the Challenge extension from the Registration Request without disturbing the authentication value used for the computation. If the Mobile-AAA Authentication extension is present and a security association exists between the foreign agent and the home agent, the Mobile-Foreign Challenge extension and the Mobile-AAA Authentication extension MUST precede the Foreign-Home Authentication extension.

If the foreign agent does remove the Challenge extension and applicable authentication from the Registration Request message, then it SHOULD store the Identification field from the Registration Request message as part of its record-keeping information about the particular mobile node in order to protect against replays.

3.2.1. Foreign Agent Algorithm for Tracking Used Challenges

If the foreign agent maintains a large CHALLENGE_WINDOW, it becomes more important for scalability purposes to efficiently compare incoming challenges against the set of Challenge values which have been advertised recently. This can be done by keeping the Challenge values in order of advertisement, and by making use of the mandated behavior that mobile nodes MUST NOT use Challenge values which were advertised before the last advertised Challenge value that the mobile node has attempted to use. The pseudo-code in Appendix E accomplishes this objective. The maximum amount of total storage required by this algorithm is equal to Size*(CHALLENGE_WINDOW + (2*N)), where N is the current number of mobile nodes for which the foreign agent is storing challenge values. Note that, whenever the stored challenge value is no longer in the CHALLENGE_WINDOW, it can be deleted from the foreign agent's records, perhaps along with all other registration information for the mobile node if it is no longer registered.

It is presumed that the foreign agent keeps an array of advertised Challenges, a record of the last advertised challenge used by a mobile node, and also a record of the last challenge provided to a mobile node in a Registration Reply or unicast Agent Advertisement.

To meet the security obligations outlined in Section 12, the foreign agent SHOULD use one of the already stored, previously unused challenges when responding to an unauthenticated Registration Request or Agent Solicitation. If none of the already stored challenges are previously unused, the foreign agent SHOULD generate a new challenge, include it in the response, and store it in the per-Mobile data structure.

3.3. Foreign Agent Processing of Registration Replies

The foreign agent SHOULD include a new Mobile-Foreign Challenge Extension in any Registration Reply, successful or not. If the foreign agent includes this extension in a successful Registration Reply, the extension SHOULD precede a Mobile-Foreign authentication extension if present. Suppose the Registration Reply includes a Challenge extension from the home agent, and the foreign agent wishes to include another Challenge extension with the Registration Reply for use by the mobile node. In that case, the foreign agent MUST

delete the Challenge extension from the home agent from the Registration Reply, along with any Foreign-Home authentication extension, before appending the new Challenge extension to the Registration Reply.

One example of a situation where the foreign agent MAY omit the inclusion of a Mobile-Foreign Challenge extension in the Registration Reply would be when a new challenge has been multicast recently.

If a foreign agent has conditions in which it omits the inclusion of a Mobile-Foreign Challenge extension in the Registration Reply, it still MUST respond with an agent advertisement containing a previously unused challenge in response to a subsequent agent solicitation from the same mobile node. Otherwise (when the said conditions are not met) the foreign agent MUST include a previously unused challenge in any Registration Reply, successful or not.

If the foreign agent does not remove the Challenge extension from the Registration Request received from the mobile node then the foreign agent SHOULD store the Challenge value as part of the pending registration request list [RFC3344]. Also, if the Registration Reply coming from the home agent does not include the Challenge extension, the foreign agent SHOULD NOT reject the Registration Request message. If the Challenge Extension is present in the Registration Reply, it MUST be the same Challenge value that was included in the Registration Request. If the Challenge value differs in the Registration Reply received from the home agent, the foreign agent MUST insert an FA Error extension with Status value HA_WRONG_CHALLENGE in the Registration Reply sent to the mobile node (see Section 10).

A mobile node MUST be prepared to use a challenge from a unicast or multicast Agent Advertisement in lieu of one returned in a Registration Reply, and MUST solicit for one if it has not already received one in a Registration Reply.

If the foreign agent receives a Registration Reply with the Code value HA_BAD_AAA_AUTH, the Registration Reply with this Code value MUST be relayed to the mobile node. In this document, whenever the foreign agent is required to reject a Registration Request, it MUST put the given code in the usual Code field of the Registration Reply, unless the Registration Reply has already been received from the home agent. In this case the foreign agent MUST preserve the value of the Code field set by the home agent and MUST put its own rejection code in the Status field of the FA Error extension (defined in [FAERR]).

3.4. Home Agent Processing of Challenge Extensions

If the home agent receives a Registration Request with the Mobile-Foreign Challenge extension, and recognizes the extension, the home agent MUST include the Challenge extension in the Registration Reply. The Challenge extension MUST be placed after the Mobile-Home authentication extension, and the extension SHOULD be authenticated by a Foreign-Home Authentication extension.

The home agent may receive a Registration Request with the Mobile-AAA Authentication extension. If the Mobile-AAA Authentication extension is used by the home agent as an authorization-enabling extension and the verification fails due to incorrect authenticator, the home agent MAY reject the Registration Reply with the error code HA_BAD_AAA_AUTH.

Since the extension type for the Challenge extension is within the range 128-255, the home agent MUST process such a Registration Request even if it does not recognize the Challenge extension [RFC3344]. In this case, the home agent will send a Registration Reply to the foreign agent that does not include the Challenge extension.

3.5. Mobile Node Processing of Registration Replies

A mobile node might receive the error code in the Registration Reply from the foreign agent as a response to the Registration Request. The error codes are defined in Section 10.

In any case, if the mobile node attempts to register again after such an error, it MUST use a new Challenge value in such a registration, obtained either from an Agent Advertisement, or from a Challenge extension to the Registration Reply containing the error.

In the co-located care-of address mode, the mobile node receives a Registration Reply without the Challenge extension and processes the Registration Reply as specified in [RFC3344]. In this case, the Challenge value 0 is recommended for the authenticator computation mentioned in Section 8.

4. Mobile-Foreign Challenge Extension

This section specifies a new Mobile IP Registration extension that is used to satisfy a Challenge in an Agent Advertisement. The Challenge extension to the Registration Request message is used to indicate the challenge that the mobile node is attempting to satisfy.

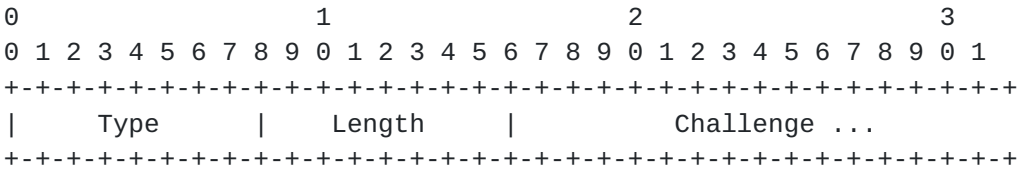

Figure 2: The Mobile-Foreign Challenge Extension

Type:

132 (skippable) (see [RFC3344])

Length:

Length of the Challenge value

Challenge:

The Challenge field is copied from the Challenge field found in the received Challenge extension.

Suppose the mobile node has successfully registered using one of the Challenge Values within the CHALLENGE_WINDOW values advertised by the foreign agent. In that case, in any new Registration Request the mobile node MUST NOT use any Challenge Value which was advertised by the foreign agent before the Challenge Value in the mobile node's last Registration Request.

5. Generalized Mobile IP Authentication Extension

Several new authentication extensions have been designed for various control messages proposed for extensions to Mobile IP. A new authentication extension is required for a mobile node to present its credentials to any other entity other than the ones already defined; the only entities defined in the base Mobile IP specification [RFC3344] are the home agent and the foreign agent. The purpose of the generalized authentication extension defined here is to collect together data for all such new authentication applications into a single extension type with subtypes.

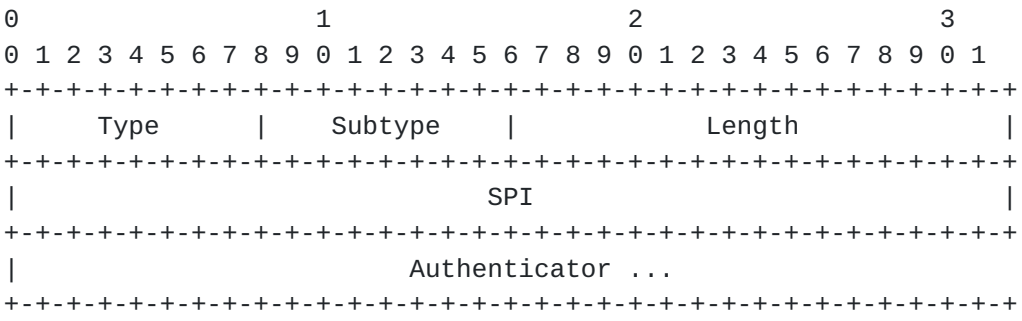

Figure 3: The Generalized Mobile IP Authentication Extension

Type:

36 (not skippable) (see [RFC3344])

Subtype:

A number assigned to identify the kind of endpoints or other characteristics of the particular authentication strategy

Length:

4 plus the number of bytes in the Authenticator; MUST be at least 20.

SPI:

Security Parameters Index

Authenticator:

The variable length Authenticator field

In this document, only one subtype is defined:

1 Mobile-AAA Authentication subtype (see Section 6)

6. Mobile-AAA Authentication subtype

The Generalized Authentication extension with subtype 1 will be referred to as a Mobile-AAA Authentication extension. The mobile node MAY include a Mobile-AAA Authentication extension in any Registration Request. This extension MAY co-exist in the same Registration Request with Authentication extensions defined for Mobile IP Registration ([RFC3344]). If the mobile node does not include a Mobile-Foreign Authentication extension, then it MUST include the Mobile-AAA Authentication extension whenever the Challenge extension is present. If both are present, the Mobile-AAA Authentication extension MUST precede the Mobile-Foreign Authentication extension.

If the Mobile-AAA Authentication extension is present, the Mobile-Home Authentication Extension MUST appear prior to the Mobile-AAA Authentication extension. The corresponding response MUST include the Mobile-Home Authentication Extension, and MUST NOT include the Mobile-AAA Authentication Extension.

The default algorithm for computation of the authenticator is HMAC-MD5 [RFC2104] computed on the following data, in the order shown:

```
Preceding Mobile IP data || Type, Subtype, Length, SPI
```

where the Type, Length, Subtype, and SPI are as shown in Section 5. The Preceding Mobile IP data refers to the UDP payload (the Registration Request or Registration Reply data) and all prior Extensions in their entirely. The resulting function call, as described in [RFC2104], would be:

```
hmac_md5(data, datalen, Key, KeyLength, authenticator);
```

Each mobile node MUST support the ability to produce the authenticator by using HMAC-MD5 as shown. Just as with Mobile IP, it must be possible to configure the use of any arbitrary 32-bit SPI outside of the SPIs in the reserved range 0-255 for selection of this default algorithm.

7. Reserved SPIs for Mobile IP

Mobile IP defines several authentication extensions for use in Registration Requests and Replies. Each authentication extension carries a Security Parameters Index (SPI) which should be used to index a table of security associations. Values in the range 0 - 255 are reserved for special use. A list of reserved SPI numbers is to be maintained by IANA at the following URL:

http://www.iana.org/numbers.html

8. SPIs for RADIUS AAA Servers

Some AAA servers only admit a single security association, and thus do not use the SPI numbers for Mobile IP authentication extensions for use when determining the security association that would be necessary for verifying the authentication information included with the Authentication extension.

SPI number CHAP_SPI (see Section 9) is reserved for indicating the following procedure for computing authentication data (called the "authenticator"), which is used by many RADIUS servers [RFC2138] today.

To compute the authenticator, apply MD5 [RFC1321] computed on the following data, in the order shown:

```
High-order byte from Challenge || Key ||

MD5(Preceding Mobile IP data ||

Type, Subtype (if present), Length, SPI) ||

Least-order 237 bytes from Challenge
```

where the Type, Length, SPI, and possibly Subtype, are the fields of the authentication extension in use. For instance, all four of these fields would be in use when SPI == CHAP_SPI is used with the Generalized Authentication extension. Also, in case of co-located care-of address, the Challenge value 0 is used (refer Section Section 3.5). Since the RADIUS protocol cannot carry attributes of length greater than 253, the preceding Mobile IP data, type, subtype (if present), length and SPI are hashed using MD5. Finally, the least significant 237 bytes of the challenge are concatenated. If the challenge has fewer than 238 bytes, this algorithm includes the high-order byte in the computation twice, but ensures that the challenge is used exactly as is. Additional padding is never used to increase the length of the challenge; the input data is allowed to be shorter than 237 bytes long.

9. Configurable Parameters

Every Mobile IP agent supporting the extensions defined in this document SHOULD be able to configure each parameter in the following table. Each table entry contains the name of the parameter, the default value, and the section of the document in which the parameter first appears.

Parameter Name	Default Value	Section of Document
CHALLENGE_WINDOW	2	3.2
CHAP_SPI	2	8

Table 1: Configurable Parameters

Note that CHALLENGE_WINDOW SHOULD be at least 2. This makes it far less likely that mobile nodes will register using a Challenge value that is outside the set of values allowable by the foreign agent.

10. Error Values

Each entry in the following table contains the name of the Code [RFC3344] to be returned in a Registration Reply, the value for the Code, and the section in which the error is mentioned in this specification.

Error Name	Value	Section of Document
UNKNOWN_CHALLENGE	104	3.2
BAD_AUTHENTICATION	67	3.2 - also see [RFC3344]
MISSING_CHALLENGE	105	3.1, 3.2
STALE_CHALLENGE	106	3.2
FA_BAD_AAA_AUTH	TBD	3.2
HA_BAD_AAA_AUTH	TBD	3.4
HA_WRONG_CHALLENGE	TBD	3.2

Table 2: Error Values

11. IANA Considerations

The following are currently assigned by IANA for RFC 3012 ([RFC3012]) which are applicable to this document. IANA should record these values as part of this document.

The Generalized Mobile IP Authentication extension defined in Section Section 5 is a Mobile IP registration extension. IANA has assigned a value of 36 for this extension.

A new number space is to be created for enumerating subtypes of the Generalized Authentication extension (see section Section 5). New subtypes of the Generalized Authentication extension, other than the number (1) for the MN-AAA authentication extension specified in section Section 6, must be specified and approved by a designated expert.

The MN-FA Challenge extension defined in Section Section 4 is a router advertisement extension as defined in RFC 1256 [[RFC1256]] and extended in RFC 3344 [[RFC3344]]. IANA should assign a value of 132 for this purpose.

The Code values defined in section Section 10 are error codes as defined in RFC 3344 ([RFC3344]). They correspond to error values conventionally associated with rejection by the foreign agent (i.e., values from the range 64-127). The Code value 67 is a pre-existing value which is to be used in some cases with the extension defined in this specification. IANA should record the values as defined in section Section 10.

A new section for enumerating algorithms identified by specific SPIs within the range 0-255 is added by IANA. The CHAP_SPI number (2) discussed in section Section 8 is assigned from this range of reserved SPI numbers. New assignments from this reserved range must be specified and approved by the Mobile IP working group. SPI number 1 should not be assigned unless in the future the Mobile IP working group decides that SKIP is not important for enumeration in the list of reserved numbers. SPI number 0 should not be assigned.

Additionally, new error codes FA_BAD_AAA_AUTH, HA_BAD_AAA_AUTH, and HA_WRONG_CHALLENGE are defined by this document. Among these, HA_WRONG_CHALLENGE may appear in the Status code of the FA Error extension defined in [FAERR].

12. Security Considerations

In the event that a malicious mobile node attempts to replay the authenticator for an old Mobile-Foreign Challenge, the foreign agent would detect it since the agent always checks whether it has recently advertised the Challenge (see Section 3.2). Allowing mobile nodes with different IP addresses or NAIs to use the same Challenge value does not represent a security vulnerability, because the authentication data provided by the mobile node will be computed over data that is different (at least the mobile nodes' IP address will vary).

If the foreign agent chooses a Challenge value (see Section 2) with fewer than 4 bytes, the foreign agent SHOULD include the value of the Identification field in the records it maintains for the mobile node. The foreign agent can then determine whether the Registration messages using the short Challenge value are in fact unique, and thus assuredly not replayed from any earlier registration.

Section 8 (SPI For RADIUS AAA Servers) defines a method of computing the Generalized Mobile IP Authentication Extension's authenticator field using MD5 in a manner that is consistent with RADIUS [RFC2138]. The use of MD5 in the method described in Section 8 is less secure than HMAC-MD5 [RFC2104], and MUST be avoided whenever possible.

Note that an active attacker may try to prevent successful registrations by sending a large number of Agent Solicitations or bogus Registration Requests, each of which could cause the foreign agent to respond with a fresh challenge, invalidating the challenge that the MN is currently trying to use. To prevent such attacks, the foreign agent MUST NOT invalidate previously unused challenges when responding to unauthenticated Registration Requests or Agent Solicitations. In addition, the foreign agent MUST NOT allocate new storage when responding to such messages, because this would also create the possibility of denial of service.

The Challenge extension specified in this document need not be used for co-located care-of address mode. In this case, replay protection is provided by the Identification field in the Registration Request message [RFC3344].

13. Acknowledgments

The authors would like to thank Pete McCann, Ahmad Muhanna, Henrik Levkowetz, Kent Leung, Alpesh Patel, Madjid Nakhjiri, Gabriel Montenegro, Jari Arkko and other MIP4 WG participants for their useful discussions.

14. Normative References

[FAERR] Perkins, C., "Foreign Agent Error Extension for Mobile IPv4", draft-perkins-mip4-faerr-02.txt (work in progress), January 2004.

[RFC1256] Deering, S., "ICMP Router Discovery Messages", RFC 1256, September 1991.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[RFC1750] Eastlake, D., Crocker, S., and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[RFC1994] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2138] Rigney, C., Rigney, C., Rubens, A., Simpson, W., and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[RFC2794] Calhoun, P. and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, March 2000.

[RFC3012] Perkins, C. and P. Calhoun, "Mobile IPv4 Challenge/ Response Extensions", RFC 3012, November 2000.

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

Appendix A. Change History

The following is the list of changes from RFC 3012 ([RFC3012]):

- Foreign agent recommended to include a Challenge in every Registration Reply, so that mobile node can re-register without waiting for an Advertisement.

- Foreign agent MUST record applicable challenge values used by each mobile node.

- Mobile node forbidden to use Challenge values which were advertised previous to the last Challenge value which it had used for a registration.

- Challenge definitions are cleaned up.

- Programming suggestion added as an appendix.

- HMAC_CHAP_SPI option is added for Generalized Mobile IP Authentication extension. Upon receipt of HMAC_CHAP_SPI, HMAC-MD5 is used instead of MD5 for computing the authenticator.

- Added FA_BAD_AAA_AUTH and HA_BAD_AAA_AUTH error codes to report authentication errors caused while processing Mobile-AAA Authentication extension. Also, added the error code HA_WRONG_CHALLENGE to indicate that Challenge value differs in the Registration Reply received from the home agent compare to the one sent to the home agent in the Registration Request.

- Processing of the Mobile-AAA Authentication extension is clarified for the foreign agent and the home agent.

- Co-existence of the Mobile-AAA Authentication extension in the same Registration Request is made explicit.

- The situation in which the foreign agent sets MISSING_CHALLENGE is clarified further.

- The use of Mobile-AAA Authentication Extension is allowed by the mobile node with co-located care-of address.

- Added protection against bogus Registration Reply and Agent Advertisement. Also, the processing of the Challenge is clarified if it is received in the multicast/unicast Agent Advertisement.

- Added reference of FA Error extension in the References section and also updated relevant text in section 3.2 and section 11.

Appendix B. Verification Infrastructure

The Challenge extensions in this protocol specification are expected to be useful to help the foreign agent manage connectivity for visiting mobile nodes, even in situations where the foreign agent does not have any security association with the mobile node or the mobile node's home agent. In order to carry out the necessary authentication, it is expected that the foreign agent will need the assistance of external administrative systems, which have come to be called AAA systems. For the purposes of this document, we call the external administrative support the "verification infrastructure". The verification infrastructure is described to motivate the design of the protocol elements defined in this document, and is not strictly needed for the protocol to work. The foreign agent is free to use any means at its disposal to verify the credentials of the mobile node. This could, for instance, rely on a separate protocol between the foreign agent and the Mobile IP home agent, and still be completely invisible to the mobile node.

In order to verify the credentials of the mobile node, we assume that the foreign agent has access to a verification infrastructure that can return a secure notification to the foreign agent that the authentication has been performed, along with the results of that authentication. This infrastructure may be visualized as shown in Figure 4.

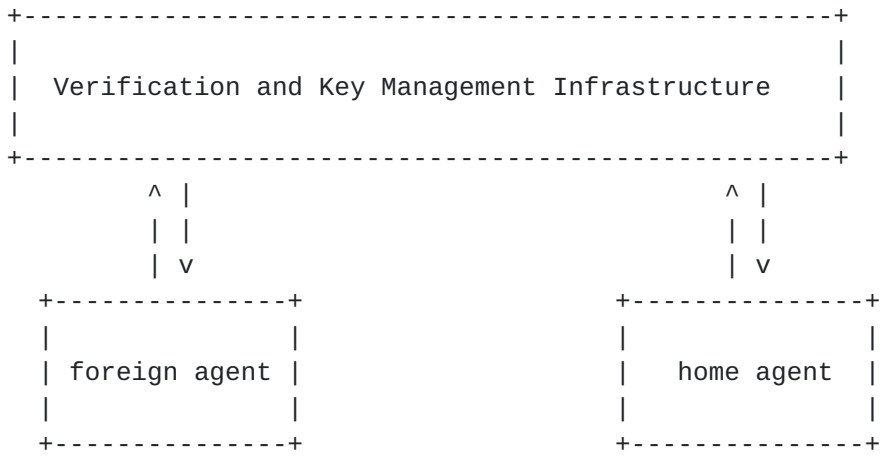

Figure 4: The Verification Infrastructure

After the foreign agent gets the Challenge authentication, it MAY pass the authentication to the (here unspecified) infrastructure, and await a Registration Reply. If the Reply has a positive status (indicating that the registration was accepted), the foreign agent

accepts the registration. If the Reply contains the Code value BAD_AUTHENTICATION (see Section 10), the foreign agent takes actions indicated for rejected registrations.

Implicit in this picture, is the important observation that the foreign agent and the home agent have to be equipped to make use of whatever protocol is made available to them by the challenge verification and key management infrastructure shown in the figure.

The protocol messages for handling the authentication within the verification infrastructure, and identity of the agent performing the verification of the foreign agent challenge, are not specified in this document, because those operations do not have to be performed by any Mobile IP entity.

Appendix C. Message Flow for FA Challenge Messaging with Mobile-AAA Extension

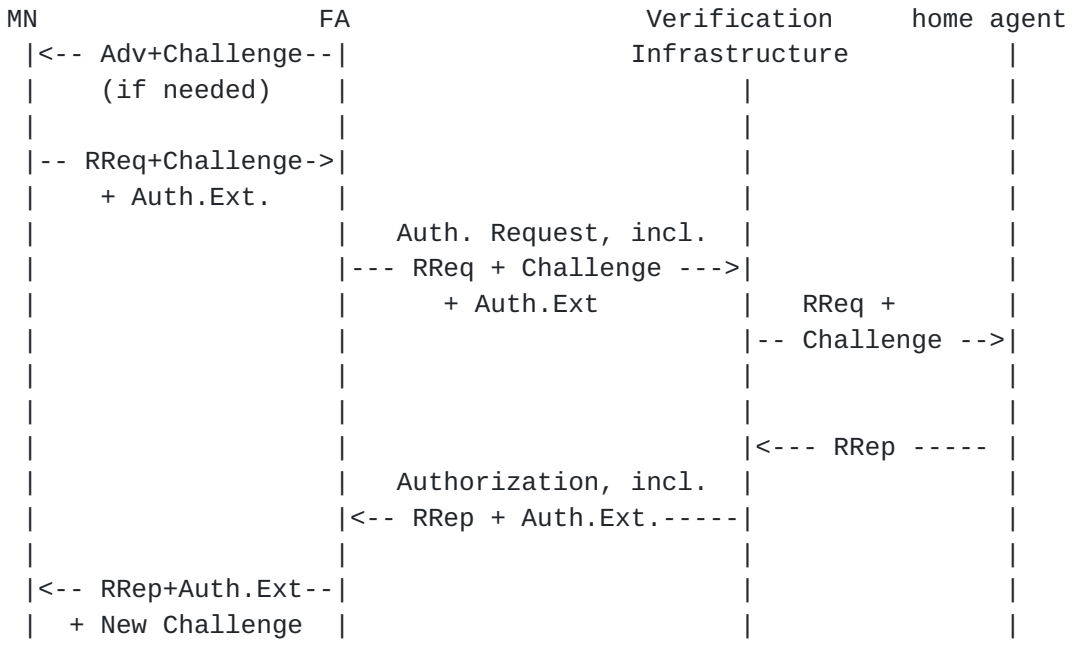

Figure 5: Message Flows for FA Challenge Messaging

In Figure 5, the following informational message flow is illustrated:

1. The foreign agent includes a Challenge Value in a unicast Agent Advertisement if needed. This advertisement MAY have been produced after receiving an Agent Solicitation from the mobile node (not shown in the diagram).

2. The mobile node creates a Registration Request including the advertised Challenge Value in the Challenge extension, along with an Mobile-AAA authentication extension.

3. The foreign agent relays the Registration Request either to the home agent specified by the mobile node, or else to its locally configured Verification Infrastructure (see Appendix B), according to local policy.

4. The foreign agent receives a Registration Reply with the appropriate indications for authorizing connectivity for the mobile node.

5. The foreign agent relays the Registration Reply to the mobile node, possibly along with a new Challenge Value to be used by the

mobile node in its next Registration Request message.

Appendix D. Message Flow for FA Challenge Messaging with MN-FA Authentication

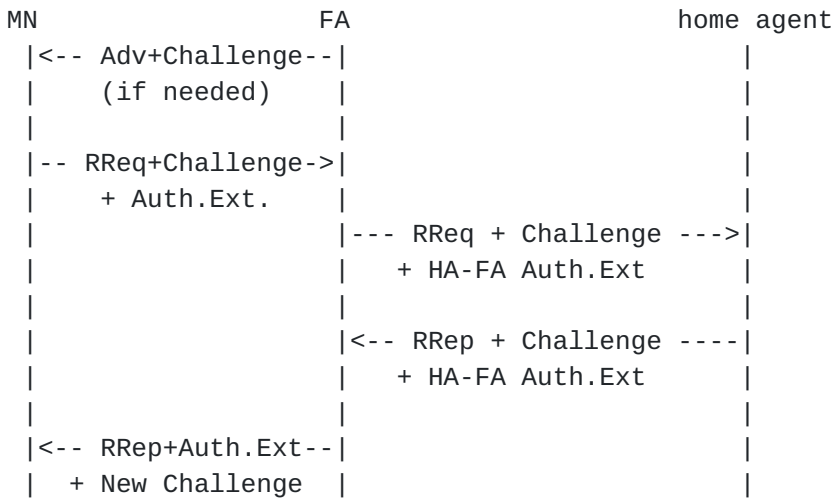

Figure 6: Message Flows for FA Challenge Messaging with MN-FA Authentication

In Figure 6, the following informational message flow is illustrated:

1. The foreign agent disseminates a Challenge Value in an Agent Advertisement if needed. This advertisement MAY have been produced after receiving an Agent Solicitation from the mobile node (not shown in the diagram).

2. The mobile node creates a Registration Request including the advertised Challenge Value in the Challenge extension, along with an Mobile-Foreign Authentication extension.

3. The foreign agent relays the Registration Request to the home agent specified by the mobile node.

4. The foreign agent receives a Registration Reply with the appropriate indications for authorizing connectivity for the mobile node.

5. The foreign agent relays the Registration Reply to the mobile node, possibly along with a new Challenge Value to be used by the mobile node in its next Registration Request message. If the Reply contains the Code value HA_BAD_AAA_AUTH (see Section 10), the foreign agent takes actions indicated for rejected registrations.

Appendix E. Example Pseudo-Code for Tracking Used Challenges

```
current_chal := RegistrationRequest.challenge_extension_value
last_chal := mobile_node_record.last_used_adv_chal

if (current_chal == mobile_node_record.RegReply_challenge) {
    update (mobile_node_record, current_chal)
    return (OK)
}
else if (current_chal "among" VALID_ADV_CHALLENGES[]{
   if (last_chal "among" VALID_ADV_CHALLENGES[]) {
      if (current_chal is "before" last_chal) {
          send_error(STALE_CHALLENGE)
          return (FAILURE)
      }
      else {
          update (mobile_node_record, current_chal)
          return (OK)
      }
   }
   else {
      update (mobile_node_record, current_chal)
      return (OK)
   }
}
else {
   send_error(UNKNOWN_CHALLENGE);
}
```

Authors' Addresses

Charles E. Perkins
Nokia Research Center
Communications Systems Lab
313 Fairchild Drive
Mountain View, California 94043

Phone: +1 650 625-2986
Email: charles.perkins@nokia.com

Pat R. Calhoun
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134

Phone: +1 408-853-5269
Email: pcalhoun@cisco.com

Jayshree Bharatia
Nortel Networks
2221, Lakeside Blvd
Richardson, TX 75082

Phone: +1 972-684-5767
Email: jayshree@nortel.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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