Mobile IP Working Group
INTERNET DRAFT
23 May 2003

Charles E. Perkins
Nokia Research Center
Pat R. Calhoun
Black Storm Networks
Jayshree Bharatia
Nortel Networks

Mobile IPv4 Challenge/Response Extensions (revised)

draft-ietf-mobileip-rfc3012bis-05.txt

Status of This Memo

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 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. This document obsoletes RFC 3012.

Contents

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 [10] 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 a use challenge/response mechanism to authenticate the mobile node. Furthermore, an addtional authentication extension, the MN-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 [1].

This document uses the term Security Parameters Index (SPI) as defined in the base Mobile IP protocol specification [7]. 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 [7]:

stale challenge
: Any challenge that has been used by the mobile node in a Registration Request message and processed by the Foreign Agent by relaying or generating a corresponding Registration Reply message. 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 [7].

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 challenge in a corresponding Registration Reply message -- 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 [4] for use by foreign agents that need to issue a challenge for authenticating mobile nodes.

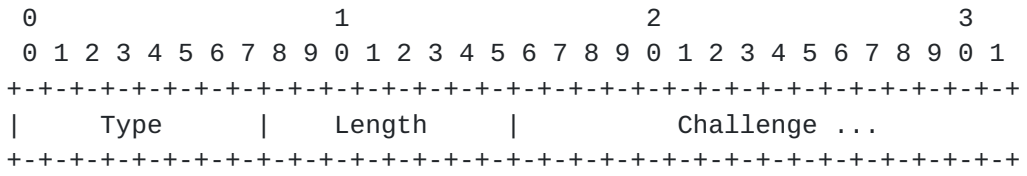

Figure 1: The Challenge Extension

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 the latest 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. [5] 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.

3. Operation

This section describes modifications to the Mobile IP registration process [7] 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 for Registration Requests

Retransmission behavior for Registration Requests is identical to that specified in Mobile IP specification [7]. 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 [7]. 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 present, the Mobile-AAA extension MUST precede to 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. In addition, the Mobile Node SHOULD include the NAI extension [2], to enable the foreign agent to make use of any available verification infrastructure. 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 or HMAC_CHAP_SPI (see section 9), then the mobile node specifies CHAP-style authentication [10] using MD5 [9] or HMAC_MD5, respectively.

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.

Based on local policy, a Mobile Node with co-located care-of-address MAY include the Mobile-AAA Authentication extension in Registration Request. In this case, if the Mobile Node uses SPI value of CHAP_SPI or HMAC_CHAP_SPI (section 8) in the MN-AAA Authentication extension, Mobile Node MUST include the Mobile-Foreign Challenge extension prior

to the Mobile-AAA Authentication extension. The mechanism used by

the Mobile Node to obtain the Challenge value is outside the scope of this document.

3.2. Foreign Agent Processing for Registration Requests

Upon receipt of the Registration Request, if the Foreign Agent has issued a Challenge as part of its Agent Advertisements, and 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 to the mobile node with the Code value MISSING_CHALLENGE.

A foreign agent that sends Agent Advertisements containing a Challenge value MAY send a Registration Reply message with a MISSING_CHALLENGE error if the mobile node sends a Registration Request with a Mobile-Foreign Authentication extension without including a Challenge. In other words, such a foreign agent MAY refuse to process a Registration Request from the mobile node unless the request contains an unused 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 [2]) are the same as represented in the visitor list entry for the pending Registration Request (section 3.7.1 of [7]). 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 last Registration Reply issued 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 appendix E 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 BAD_AAA_AUTHENTICATION_SET_BY_FA. 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. 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, the Foreign Agent MAY remove the Challenge Extension from the Registration Request without disturbing the authentication value computed by the Mobile Node for use by the AAA or the Home Agent. If the Challenge extension is not removed, it MUST precede the Foreign-Home Authentication extension.

If the Foreign Agent does not remove the Challenge extension, then the Foreign Agent SHOULD store the Challenge value as part of the pending registration request list [7]. Also, the Foreign Agent SHOULD NOT reject any Registration Reply message coming from the Home Agent that does not include the Challenge Extension. 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 defers in the Registration Reply

received from the Home Agent, the Foreign Agent MUST reject the Registration Request and change the status in the Registration Reply to the Code value MISSING_CHALLENGE (see section 10).

If the Foreign Agent does remove the Challenge extension and applicable authentication from the Registration Request message, then it SHOULD insert the Identification field from the Registration Request message along with its record-keeping information about the particular Mobile Node in order to protect against replays.

3.3. Foreign Agent Processing for 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. 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.

If the Foreign Agent receives a Registration Reply with the Code value BAD_AAA_AUTHENTICATION_SET_BY_HA, it MUST be relayed to the Mobile Node.

3.4. Home Agent Processing for the 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.

If the Home Agent receives a Registration Request with the Mobile-AAA Authentication extension, it will be handled based on the local policy of the Home Agent. 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 BAD_AAA_AUTHENTICATION_SET_BY_HA.

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 [7]. 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 for Registration Replies

A Mobile Node might receive the following error codes in the Registration Reply from the Foreign Agent as a response to the Registration Request. The error codes are defined in section 10.

UNKNOWN_CHALLENGE: This error code is received by the Mobile Node in the case where the Mobile Node has moved to a new Foreign Agent that cannot validate the challenge provided in the Registration Request. In such instances, the Mobile Node MUST use a new Challenge value in any new registration, obtained either from an Agent Advertisement, or from a Challenge extension to the Registration Reply containing the error.

MISSING_CHALLENGE: A Mobile Node that does not include a Challenge when the Mobile-Foreign Authentication extension is present may receive a MISSING_CHALLENGE error. In this case, the Mobile Node SHOULD send an unused Challenge extension in the next Registration Request.

BAD_AUTHENTICATION: This error is sent by the Foreign Agent if the Registration Request contains a Mobile-Foreign Authentication extension with an incorrect authenticator that fails verification. A Mobile Node that receives a BAD_AUTHENTICATION Code value SHOULD include the Mobile-AAA Authentication Extension in the next Registration Request. This will make it possible for the Foreign Agent to use its AAA infrastructure in order to authenticate the Mobile Node. In this case, the Mobile Node MUST use a new Challenge value in any new registration, obtained either from an Agent Advertisement, or from a Challenge extension to the Registration Reply containing the error.

BAD_AAA_AUTHENTICATION_SET_BY_FA: This error is sent by the Foreign Agent if the Registration Request contains a Mobile-AAA Authentication extension with an incorrect authenticator that fails verification. A Mobile Node that receives a BAD_AAA_AUTHENTICATION_SET_BY_FA MUST use a new Challenge value in any new registration, obtained either from an Agent Advertisement, or from a Challenge extension to the Registration Reply containing the error.

BAD_AAA_AUTHENTICATION_SET_BY_HA: This error is sent by the Home Agent if the Registration Request contains a Mobile-AAA Authentication extension with an incorrect authenticator

that fails verification. A Mobile Node that receives a BAD_AAA_AUTHENTICATION_SET_BY_HA MUST use a new Challenge value in any new registration, obtained either from an Agent Advertisement, or from a Challenge extension to the Registration Reply containing the error.

STALE_CHALLENGE: If the Foreign Agent receives a Registration Request with a Challenge extension containing a Challenge value previously used by that mobile node, the Mobile Node MAY receive a Registration Reply to the mobile node containing the Code value STALE_CHALLENGE. In such instances, the Mobile Node MUST use a new Challenge value in next Registration Request, obtained either from an Agent Advertisement, or from a Challenge extension to the Registration Reply containing the error.

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.

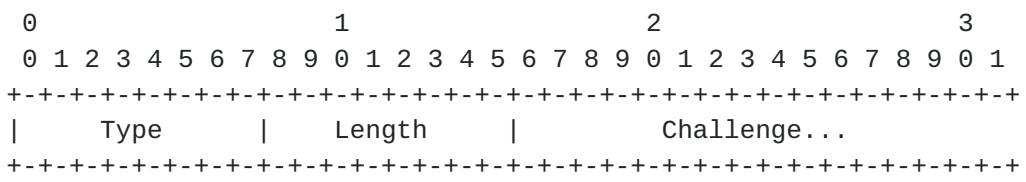

Figure 2: The Mobile-Foreign Challenge Extension

Type 132 (skippable) (see [7])

Length Length of the Challenge value

Challenge The Challenge field is copied from the Challenge field found in the Agent Advertisement Challenge extension (see section 2).

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 [7] are the home agent and the foreign agent. It is the purpose of the generalized authentication extension defined here to collect together data for all such new authentication applications into a single extension type with subtypes.

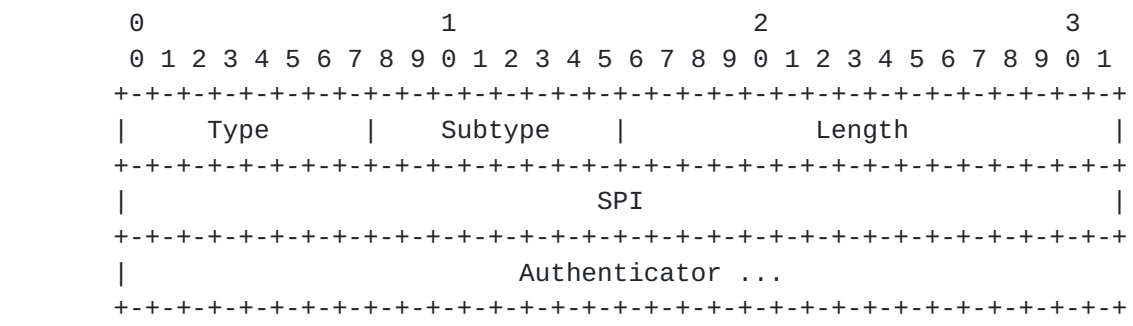

Figure 3: The Generalized Mobile IP Authentication Extension

Type	36 (not skippable) (see [7])
Subtype	a number assigned to identify the kind of endpoints or the 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 Authetication extensions defined for Mobile IP Registration by [7]. If the mobile node does not include a Mobile-Foreign Authentication [7] extension, then it MUST include the Mobile-AAA Authentication extension whenever the Challenge extension is present. If present, the Mobile-AAA extension MUST precede to the Mobile-Foreign Authentication extension.

If the Mobile-AAA Authentication extension is present, then the Registration Message sent by the mobile node MUST contain the Mobile-Home Authentication extension [7] if it shares a security association with the Home Agent. If 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 [6] 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 resulting function call, as described in [6], 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

From that URL, follow the hyperlinks to [M] within the "Directory of General Assigned Numbers", and subsequently to the specific section for "Mobile IP Numbers".

8. SPI 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 numbers CHAP_SPI and HMAC_CHAP_SPI (see section 9) are reserved for indicating the following procedure for computing authentication

data (called the "authenticator"), which is used by many RADIUS servers [8] today.

To compute the authenticator, apply MD5 [9] 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 or HMAC_CHAP_SPI) is used with the Generalized Authentication extension. However, SPI number HMAC_CHAP_SPI indicates the use of HMAC_MD5 instead of MD5 in the above procedure. Since the RADIUS protocol cannot carry attributes greater than 253 in size, 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(s) of Document
CHALLENGE_WINDOW	2	3.2
CHAP_SPI	2	8
HMAC_CHAP_SPI	3	8

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 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 of Document
UNKNOWN_CHALLENGE	104	3.2
BAD_AUTHENTICATION	67	3.2 - also see [7]
MISSING_CHALLENGE	105	3.1,3.2
STALE_CHALLENGE	106	3.2
BAD_AAA_AUTHENTICATION_SET_BY_FA	TBD	3.2
BAD_AAA_AUTHENTICATION_SET_BY_HA	TBD	3.4

11. IANA Considerations

All protocol values in this specification are to be the same as defined in RFC 3012 [3]. Additionaly, new Code values are defined by this document for BAD_AAA_AUTHENTICATION_SET_BY_FA and BAD_AAA_AUTHENTICATION_SET_BY_HA.

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 by the bytes of the mobile nodes' IP addresses).

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 [8]. The use of MD5 in the method described in Section 8 is less secure than HMAC-MD5 [6], and should be avoided whenever possible.

13. Acknowledgments

The authors would like to thank Tom Hiller, Mark Munson, the TIA TR45-6 WG, Gabriel Montenegro, Vipul Gupta, Pete McCann, Robert Marks, Ahmad Muhanna, and Luca Salgarelli for their useful discussions. A recent draft by Mohamed Khalil, Raja Narayanan, Emad Qaddoura, and Haseeb Akhtar has also suggested the definition of a generalized authentication extension similar to the specification contained in section 5.

References

[1] 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.

[2] P. Calhoun and C. Perkins. Mobile IP Network Access Identifier Extension for IPv4. Request for Comments (Proposed Standard) 2794, Internet Engineering Task Force, January 2000.

[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] S. Deering. ICMP Router Discovery Messages. Request for Comments (Proposed Standard) 1256, Internet Engineering Task Force, September 1991.

[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] C. Perkins. IP Mobility Support. Request for Comments (Proposed Standard) 3344, Internet Engineering Task Force, August 2002.

[8] 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.

[9] R. Rivest. The MD5 Message-Digest Algorithm. Request for Comments (Informational) 1321, Internet Engineering Task Force, April 1992.

[10] W. Simpson. PPP Challenge Handshake Authentication Protocol (CHAP). Request for Comments (Draft Standard) 1994, Internet Engineering Task Force, August 1996.

All references are normative.

A. Change History

List of the important changes for version 03.

- 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.

- terminology for stale challenge vs. unused challenge clarified

- terminology for "valid" challenge deleted in favor of "unused challenge"

- Programming suggestion added as an appendix

List of the important changes for version 04.

- The definition of "previously used challenge" is merged with "stale challenge" definition in section 1.1.

- Reference 7 is updated from RFC 3320 to RFC 3344 and reference 9 is updated from RFC 2138 to RFC 2865 in "Reference" section.

- Reference to RFC 3344 is added in section 3.

- 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.

- Clarified processing of error messages at the Mobile Node (section 3.1).

- Modified text of section 2.1 and 3.2 for further clarity.

List of the important changes for version 05.

- Added BAD_AAA_AUTHENTICATION_SET_BY_FA and BAD_AAA_AUTHENTICATION_SET_BY_HA error codes to report authentication errors caused while processing Mobile-AAA Authentication extension.

- Processing of the Mobile-AAA Authentication extension is clarified for the Foreign Agent and the Home Agant.

- Co-existance of the Mobile-AAA Authentication extension in the same Registration Request is made explict.

- 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.

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 imagine 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.

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

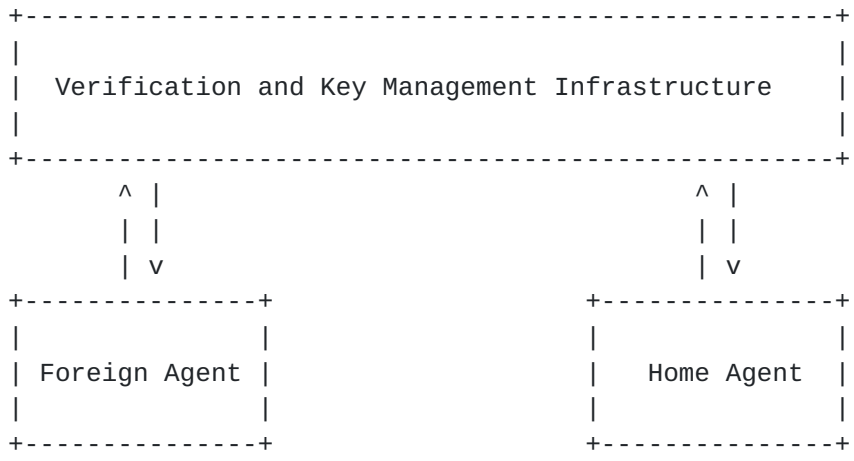

Figure 4: The Verification Infrastructure

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.

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

In figure 5, the following 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 MN-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.

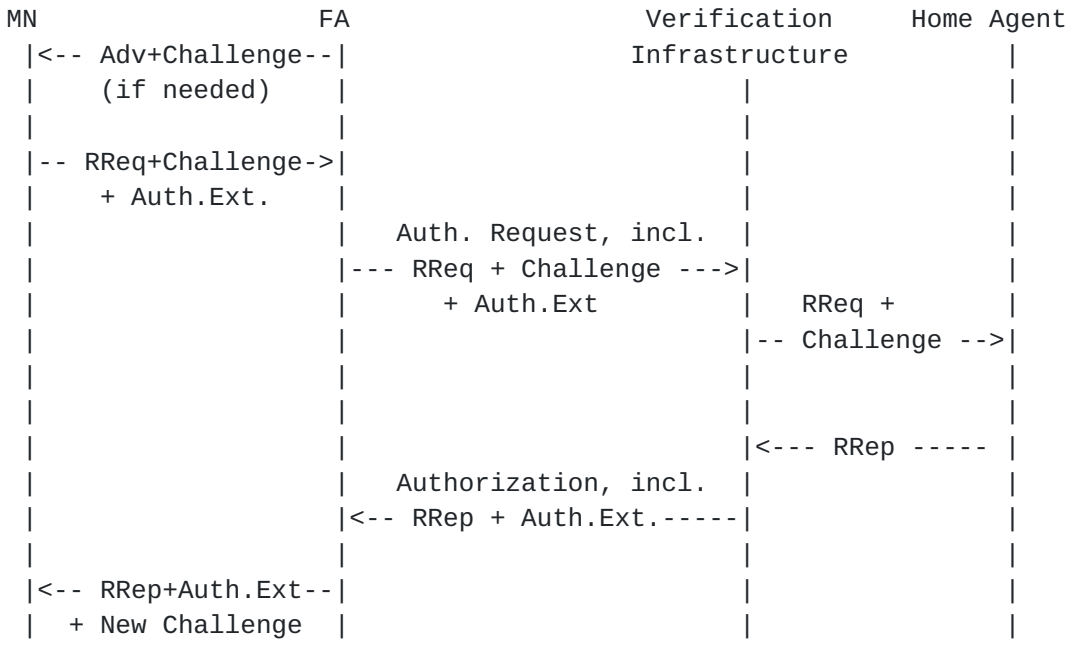

Figure 5: Message Flows for FA Challenge Messaging

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 Reply message.

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

In figure 6, the following 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 either to the home agent specified by the mobile node.

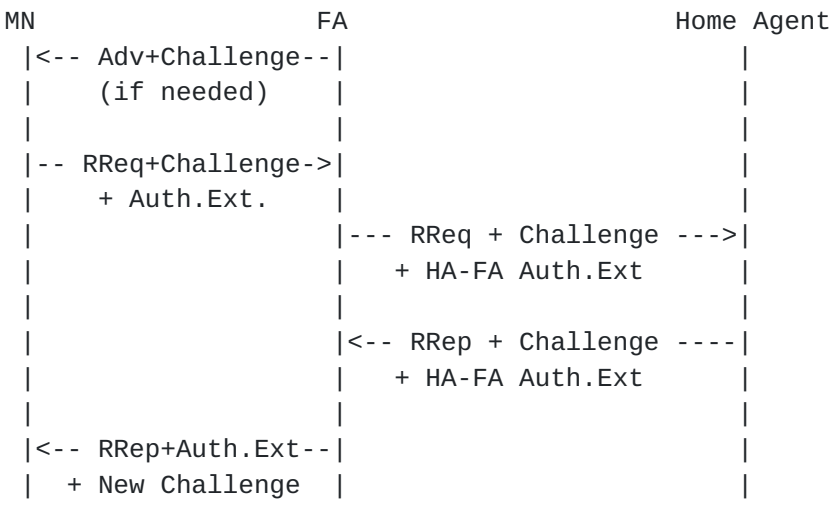

Figure 6: Message Flows for FA Challenge Messaging with MN-FA Authentication

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

E. 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 following stylized programmatic algorithm 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.

In the program fragment, it is presumed that the foreign agent keeps an array of advertised Challenges ("VALID_ADV_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.

```
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);
}
```

Addresses

Questions about this memo can 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
Airespace Networks
110 Nortech Parkway
San Jose, CA 95134
USA
Phone: +1 408 635 2000
Email: pcalhoun@diameter.org
Fax: +1 720-293-7501

Jayshree Bharatia
Nortel Networks
2221, Lakeside Blvd.
Richardson, TX, 75082
USA
Phone: +1 972-684-5767
Email: jayshree@nortelnetworks.com
Fax: +1 972-684-3775