Mobile IP Working Group Yingchun Xu
Ken Peirce
Ed Campbell
INTERNET DRAFT 3Com Corporation
Category: Internet Draft
Title: draft-ietf-mobileip-radius-challenge-00.txt
Date: June 1999

Mechanism to Support CHAP Mobile Node Authentication for RADIUS/DIAMETER Hybrid AAA Networks

<draft-ietf-mobileip-radius-challenge-00.txt>

Status of this Memo

Abstract

Mobile IP Authentication is a requirement for the TR 45.6 CDMA wireless packet data service architecture[8]. Diameter AAA, as described in [1] and [2], is used to

support Mobile IP authentication. This requires that both the foreign and home network deploy Diameter servers. Currently, RADIUS servers have been deployed and are widely used in the Internet Service Provider(ISP) arena.While DIAMETER is required to provide the advanced AAA support required by the TR 45.6 architecture, a smooth transition from RADIUS AAA to Diameter AAA is required. At a minimum,the Diameter AAA server located in a foreign network must inter-operate with RADIUS AAA located in Home Network.

In this specification, a new SPI is specified to support Home RADIUS and Foreign DIAMETER AAA interaction. The specification requires extensions as specified in [6].

Applicability

This specification is intended for those DIAMETER servers that wish to interoperate with current RADIUS servers using PPP CHAP authentication.

1.0 Introduction

Diameter AAA, as described in [1] and [2] supports Mobile IP authentication. This requires both foreign network and home network to deploy Diameter servers. Currently, RADIUS servers have been deployed and are used widely in the Internet. To support a smooth transition from RADIUS AAA to Diameter AAA, the minimum requirement is for the Diameter AAA server located in foreign network to inter-operate with RADIUS AAA located in Home Network.

In this specification, a new SPI is specified to support Home RADIUS AAA in Mobile IP service. The specification requires extensions as specified in [6]. A default algorithm is described in [6] for computation of the authenticator field from the MN-AAA Authentication Extension. The default algorithm calculates the authenticator by using MD5 in "prefix+suffix" mode.In this specification, a new SPI is specified to support CHAP authentication. This algorithm calculates the MN-AAA authenticator field by using MD5 in "Prefix Only" mode.

2.0 Conventions

The following language conventions are used in the items of specification in this document:

- MUST, SHALL, or MANDATORY -- This item is an absolute requirement of the specification.

o SHOULD or RECOMMEND -- This item should generally be followed for all but exceptional circumstances.

o MAY or OPTIONAL -- This item is truly optional and may be followed or ignored according to the needs of the implementor.

3.0 Acronynms ,sp1

mobile client(MC) - is a device that expects to be able to maintain a network layer connection with its "home" network despite have multiple short lived PPP connections with different Foreign Agents.

Foreign Agent(FA) - is a device that issues advertisements, via its PPP links with mobile nodes, that indicate its willingness to act as an endpoint for a mobile IP tunnel. Foreign Agents can change as the mobile node moves between different regions.

Home Agent(HA) - is a device that maintains the connection with the mobile node througout the mobile IP session.

Radio Network(RN) - The radio portion of the CDMA cellular network.

4.0 Problem Space Overview

In this section we describe in high level terms the scope of the problem being addressed.The two most likely scenarios to encounter the problem are shown below. Figure 1 depicts a mobile client(MC) connecting through a radio network(RN) to a Mobile IP foreign agent(FA). The FA uses a series of DIAMETER servers to handle the authorization, acquisition of the client profile (QoS level etc.) , of the MC. The final DIAMETER stage of the DIAMETER server chain is called a broker. It is called a broker because it handles MIP sessions for multiple Home networks. For example, a major carrier could offer connectivity for multiple ISPs.(The CDMA and Broker networks could belong to the same entity.) The Broker interacts with the Home network's RADIUS server to obtain the required client records.

Figure 2 depicts a similar scenario with the Home agent functionality also out-sourced by the broker network. Note that in both cases the RADIUS server is maintained by the Home network. This allows the Home network operator to maintain control over Home network access and relieves the Broker from having to maintain client records.

Topologies:

| |

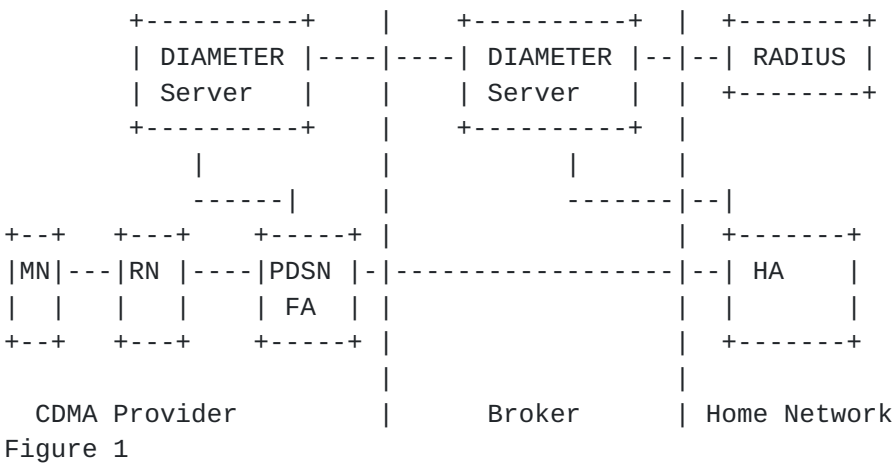

Figure 1

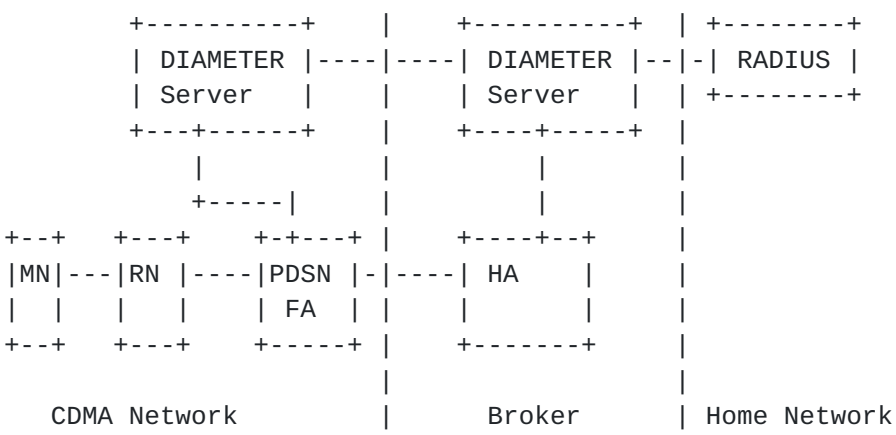

Figure 2

The problem is that the CHAP authentication mechanism defined for MIP differs from that of RADIUS.Therefore, when the broker DIAMETER server attempts to perform a CHAP proxy authentication with the Home network RADIUS server, it will fail.

5.0 Challenge/Response Authentication Calculation Parameter Mis-match

In [6],the Challenge/Response mechanism has been used to support Foreign Agent Authentication and Authorization. RADIUS based CHAP protocol also uses the Challenge/Response mechanism.

The RADIUS server calculates the authenticator using MD5 on the following data:
CHAP ID octet, KEY (or shared secret), CHAP challenge.

In [6], the Authenticator field from MC-AAA extension is calculated by using MD5 in prefix + suffix mode over following data:

Key || Preceding Mobile IP data || Type, Length, SPI || Key

This difference in the inputs to the hash function is what causes the interoperability problem. In order to use CHAP and inter-operate with RADIUS AAA, the MN-AAA extension is defined as follows:

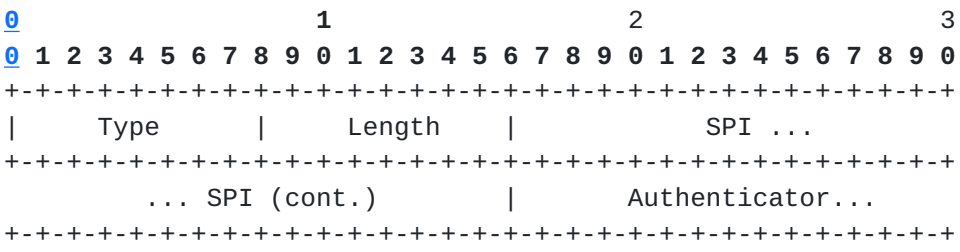

Figure 3: The MN-AAA Authentication Extension

Type	36 (not skippable)
Length	4 plus the number of bytes in the Authenticator, MUST be at least 20.
SPI	Security Parameters Index - TBD
Authenticator	The variable length Authenticator field consists of a random value of at least 128 bits.

The algorithm for computation of the authenticator is MD5 [5] computed on the following data, in the order shown:

Challenge-Octet || Key || Preceding Mobile IP data || Type, Length, SPI

The Type, Length, and SPI are as shown above. The Challenge-Octet is the last octet of the FA Challenge value from the FA Challenge Extension.

Each mobile node MUST support the ability to produce the authenticator by using MD5 as described above in order to support Home RADIUS authentication. Again this is different from the default algorithm as described in [6], which uses MD5 in "prefix+suffix" mode.

6.0 Operation

In order to use a Home RADIUS server with a Diameter AAA server for the first time Mobile IP registration authentication as described in [1] and [2], the Mobile Node and its corresponding Broker Diameter server will be configured with the new SPI as described above. It is called the "RADIUS Authentication SPI"

When a Mobile Node receives an Agent Advertisement message, it MUST use the "RADIUS Authentication SPI" and the corresponding algorithm to construct its Mobile Registration Request message if RADIUS/DIAMETER CHAP authentication interoperation is required..

The FA will then send an AA-Mobile-Node-Request(AMR) message to the Diameter AAA located in its serving network.

The Serving Diameter AAA server will then use the NAI extension to locate the Broker Diameter AAA server and forward it the AMR message.

The Broker Diameter AAA server MUST then generate a RADIUS Access-Request message based on the MN-AAA Authentication extension and the NAI extension. This message MUST then be sent to the Home RADIUS server.

The Access-Request message MUST be constructed as follows:

The CHAP-ID octet of the RADIUS CHAP-password attribute will contain the last byte of the Challenge value from MIP FA Challenge extension[6]. The authenticator from the MN-AAA Authentication extension MUST be used as the CHAP-Password attribute. The User-Name attribute MUST be populated with the user-name attribute from the AMR message. The following data stream, as described earlier, MUST be included in the CHAP-Challenge attribute:

Preceding Mobile IP data || Type, Length, SPI.

The RADIUS server now looks up a password based on the User-Name. It then encrypts the challenge using MD5 on:

CHAP ID octet, locally stored password for this specific User-Name, the CHAP challenge (from the CHAP-Challenge attribute if present,otherwise from the Request Authenticator),

The RADIUS server then compares this result with the CHAP-Password(MN-AAA Authentication extension authenticator). If these values match, the server MUST send back a RADIUS Access-Accept, otherwise it MUST send back a RADIUS Access-Reject. See [7] for details.

Upon receipt of a RADIUS Access-Accept message, the Broker Diameter AAA server MUST generate a Home Agent MIP Request(HAR)[1] and send it to the Home Agent. See [1] and [2] for rest of the operation.

Upon receipt of a RADIUS Access-Reject message, the Broker

Diameter AAA server MUST generate an AA-Mobile-Node-Answer(AMA)[1] with a result and send it back to serving Diameter AAA server as described in [1] and [2].

7.0 References

[1] P. Calhoun and C. E. Perkins. DIAMETER Mobile IP Extensions.
draft-calhoun-diameter-mobileip-01.txt, November 1998. (work in progress).

[2] P. Calhoun and A. Rubens. DIAMETER Base Protocol.
draft-calhoun-diameter-07.txt, November 1998. (work in progress).

[3] Pat R. Calhoun and Charles E. Perkins. Mobile IP Network Address Identifier Extension. draft-ietf-mobileip-mn-nai-02.txt, May 1999. (work in progress).

[4] C. Perkins, Editor. IP Mobility Support. RFC 2002, October 1996.

[5] Ronald L. Rivest. The MD5 Message-Digest Algorithm. RFC 1321, April 1992.

[6] Charles E. Perkins and Pat R. Calhoun. Mobile IP Challenge/Response Extensions.
draft-ietf-mobileip-challenge-02.txt, May 1999. (work in progress).

[7] C. Rigney, etc. Remote Authentication Dial In User Service (RADIUS),
RFC 2138, April 1997.

[8] Hiller et al., draft-hiller-3gwireless-00.txt, March 1999, (work in progress).

11.0 Author's Addresses

Kenneth Peirce, Yingchun Xu, Ed Campbell
3Com Corporation
1800 W. Central Road
Mount Prospect
Illinois 60056
kenneth_peirce@mw.3com.com, yinchung_xu@mw.3com.com, ed_campbell@mw.3com.com