Internet Engineering Task Force AAA WG
Internet Draft
Srinivas/Chan/Sengodan/Costa-Requena
draft-srinivas-aaa-basic-digest-00.txt
Nokia
July 13, 2001
Expires: Jan 13 2002

Mapping of Basic and Digest Authentication to DIAMETER AAA Messages

STATUS OF THIS MEMO

Abstract

With protocols such as SIP (RFC2543 [1]) and HTTP (RFC2616 [2]) , a AAA mechanism may be used in the back-end to handle the authentication, authorization and accounting functionality. Two authentication mechanisms specified within RFC2616 and RFC2543 are the Basic and Digest authentication. In this document, we describe how these authentication mechanisms can utilize the NASREQ application DIAMETER AAA framework.

1 Introduction

1.1 Scenario

Protocols that use Basic and Digest authentication mechanisms can benefit from a suitable mapping of such mechanisms to a AAA framework. Such protocols include HTTP and SIP. In this document, we propose a mapping between Basic/Digest authentication and a DIAMETER based AAA framework. Specifically, the NASREQ application within DIAMETER is used for this purpose.

Figure 1 depicts the scenario that is relevant for this document. It shows a generic case where entities A and B communicate in the front-end using protocols such as HTTP/SIP, while entities B and C communicate in the back-end using a AAA protocol such as DIAMETER.

```
+---+           +---+           +---+
|   |     1     |   |     2     |   |
|   |---------->|   |---------->|   |
| A |     4     | B |     3     | C |
|   |<----------|   |<--------- |   |
|   |           |   |           |   |
+---+           +---+           +---+
```

Figure 1: Scenario relevant to document

Depending on the roles played by entities A, B and C, at least four cases, as tabulated below, are possible:

	A	B	C
I)	SIP UA Client	SIP UA Server/ DIAMETER Client	DIAMETER Server
II)	SIP UA Client	SIP Proxy Server/ DIAMETER Client	DIAMETER Server
III)	HTTP Client	HTTP Server/ DIAMETER Client	DIAMETER Server
IV)	HTTP Client	HTTP Proxy Server/ DIAMETER Client	DIAMETER Server

Table 1: Roles played by Entities A,B,C in Figure 1

Other scenarios that may be possible include the case where (1) entities A and B are SIP/HTTP proxy servers, and (2) entity A is a SIP/HTTP proxy server and entity B is a SIP UA Server or HTTP origin server.

Irrespective of the roles played by entities A and B, user at A is authenticated using the DIAMETER AAA protocol. Authentication is carried out by a backend DIAMETER server C which communicates with B using the DIAMETER protocol. A principal assumption about the function of the backend server is that it is responsible for all authentication and authorization decisions. In processing a DIAMETER request, the DIAMETER server C also needs to decide what authentication scheme to use (both SIP and HTTP support Basic and Digest authentication).

1.2 Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALLNOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119.

1.3 Motivation and Approach

Basic and Digest authentication are used within protocols such as HTTP and SIP. They have also been proposed within other protocols - for instance, [3,4]. Recently, there have been efforts towards the use of an Extensible Authentication Protocol (EAP) within protocols such as HTTP and SIP. [5] is one such effort. The advantage here is that, new authentication schemes may be used without any modification to the SIP/HTTP protocol itself. This is because the EAP packet for the particular authentication scheme is carried transparently by the SIP/HTTP protocol.

However, the use of Basic and Digest authentication is likely to continue to be used directly within protocols such as SIP/HTTP in the near future, and hence their interworking with a DIAMETER AAA framework is needed.

The rest of the document is ordered as follows. Section 2 gives an overview of Basic and Digest authentication schemes, while Section 3 gives an overview of the DIAMETER protocol and the NASREQ application. Section 4 describes how Basic/Digest authentication can utilize a DIAMETER NASREQ application framework, and illustrative examples are provided.

2 Overview of Basic and Digest Authentication

HTTP and SIP both use a simple challenge-response mechanism for access authentication. Under this framework, a client issuing a request to a server MAY need to be authenticated by server using one of the authentication scheme defined. The server sends a challenge in the WWW-Authenticate header of a 401 Unauthorized response message, or Proxy-Authenticate header of a 407 Proxy Authentication Required message. Upon receiving this challenge, the client MAY resend the original request, with the appropriate credentials carried in the Authorization header if the challenge was from a 401 Unauthorized message, and in the Proxy-Authorization header if the challenge was from a 407 Proxy Authentication Required message (see section 2.3 for more details of the different cases.)

Two authentication schemes are defined for HTTP (which are also used by SIP): the Basic and Digest Authentication schemes. In the following subsections, a minimal description of these two schemes will be presented for better understanding of their mappings to Diameter messages. For full details of the schemes, please refer to RFC2617 [6].

2.1 Basic Authentication

With Basic Authentication, the challenge issued by a server is of the form:

```
      challenge   = "Basic" realm
```

An example of the WWW-Authenticate header in a 401 response message is as follows:

```
      WWW-Authenticate: Basic realm="WallyWorld"
```

Upon receiving this challenge, the client would resend the original request, with the credentials included in the Authorization header. The credentials for Basic Authentication is of the following form:

```
      credentials = "Basic" basic-credentials

      basic-credentials = base64-user-pass
```

where base64-user-pass is the base64 encoding [7] of the userid together with the password (or the form: "userid:password"). A userid of "Aladdin" and password "open sesame" results in the following Authorization header:

```
      Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

2.2 Digest Authentication

Basic Authentication is not a secure authentication scheme since the user password is sent over the network unencrypted (base64 encoding can be easily decoded.) Digest Authentication aims at improving on this major drawbacks by not sending the password in clear text, but rather through some forms of message digest mechanism. The format of a Digest challenge is:

```
      challenge         =  "Digest" digest-challenge

      digest-challenge  = 1#( realm | [ domain ] | nonce |
                            [ opaque ] |[ stale ] | [ algorithm ] |
                            [ qop-options ] | [auth-param] )
```

Among the various fields which may be present in the digest-challenge, the nonce contains a string uniquely generated by the Server for each 401 response.

The Digest response is of the form:

```
      credentials       = "Digest" digest-response
      digest-response   = 1#( username | realm | nonce | digest-uri
                          | response | [ algorithm ] | [cnonce] |
                          [opaque] | [message-qop] |
                          [nonce-count]  | [auth-param] )
```

The response is computed by the client as described in [6] and proves that the client knows the password.

2.3 Usage in HTTP and SIP

2.3.1 Usage in HTTP

Referring to Figure 1, when HTTP is being used, A is an HTTP client and B may be an HTTP server. In this case, Message 1 may be a GET request. If such a GET request contains no suitable Authorization header and if the HTTP Client A needs to be authenticated by HTTP Server B, then Message 3 would be a "401 Unauthorized" response containing a suitable WWW-Authenticate header. If the GET request contains a suitable Authorization header, then Message 3 would be a 200 OK response.

B may also be an HTTP Proxy Server. In this case, if the request in Message 1 does not contain a suitable Proxy-Authorization header and Client A needs to be authenticated by HTTP Proxy Server B, then Message 3 would be a "407 Proxy Authentication Required" response containing a suitable Proxy-Authenticate header. If the GET request

contains a suitable Proxy-Authorization header, then the HTTP Proxy Server B forwards the GET request onward..

2.3.2 Usage in SIP

The authentication mechanism of SIP resembles that of HTTP. Referring to Figure 1, when SIP is being used, A is a SIP User Agent Client (UAC) and B may be a SIP User Agent Server (UAS). In this case, Message 1 may be an INVITE request. If such an INVITE request contains no suitable Authorization header and if the SIP UAC needs to be authenticated by the SIP UAS, then Message 3 would be a "401 Unauthorized" response containing a suitable WWW-Authenticate header. If the INVITE request contains a suitable Authorization header, then Message 3 would be a 200 OK response.

Similarly, B may also be a SIP Proxy Server. In this case, if the request in Message 1 contains no suitable Proxy-Authorization header and UAC A needs to be authenticated by SIP Proxy Server B, then Message 3 would be a "407 Proxy Authentication Required" response containing a suitable Proxy-Authenticate header. If the INVITE request contains a suitable Proxy-Authorization header, then the SIP Proxy Server B forwards the SIP INVITE message onward.

3 Overview of DIAMETER

3.1 DIAMETER Framework and Base Protocol

DIAMETER was proposed as a AAA protocol, which overcomes some of the limitations of the RADIUS protocol. [8] describes the DIAMETER framework.

The DIAMETER base protocol is specified in [9], and it provides the minimum requirements needed for a AAA protocol. Its functionality includes delivery of AVPs (attribute value pairs), capabilities negotiation, error notification and extensibility. The Diameter protocol consists of a header followed by objects, which in turn are each encapsulated in a header known as an Attribute-Value-Pair (AVP).

The DIAMETER base protocol is never used on its own, but is used in conjunction with a DIAMETER application. One such DIAMETER application is NASREQ [10]. Every Diameter application specification MUST have an IANA assigned Extension-Id value.

3.2 DIAMETER NASREQ Application

The DIAMETER NASREQ application is being specified to satisfy AAA

requirements in a PPP/SLIP dialup and Terminal-Server access scenario. This application supports both legacy authentication protocols typically supported by RADIUS servers as well as PPP's Extensible Authentication Protocol (EAP). The NASREQ Extension-Id value is 1.

Two commands specified in this application, that are of relevance to this document, are the AA-Request and AA-Answer commands. In the scenario of Figure 1, Message 2 is always an AA-Request message, while Message 3 is always an AA-Answer message. The format of these messages is as follows:

```
   <AA-Request> ::= < Diameter Header: 265, REQUEST >
                    < Session-Id >
                    { Auth-Application-Id }
                    { Origin-Host }
                    { Origin-Realm }
                    { Destination-Realm }
                    { Service-Type }
                    [ Destination-Host ]
                    [ NAS-Identifier ]
                    [ User-Name ]
                    [ User-Password ]
                    [ ARAP-Password ]
                    [ CHAP-Password ]
                    [ CHAP-Challenge ]
                    [ Idle-Timeout ]
                    [ State ]
                    [ Authorization-Lifetime ]
                    [ Session-Timeout ]
                    [ Origin-State-Id ]
                    [ NAS-Key-Binding ]
                  * [ AVP ]
                  * [ Proxy-Info ]
                  * [ Route-Record ]


   <AA-Answer> ::= < Diameter Header: 265 >
                   < Session-Id >
                   { Auth-Application-Id }
                   { Result-Code }
                   { Origin-Host }
                   { Origin-Realm }
                   { Service-Type }
                   { Destination-Host }
                   [ User-Name ]
                   [ Error-Reporting-Host ]
                   [ Idle-Timeout ]
```

```
                      [ Authorization-Lifetime ]
                      [ Session-Timeout ]
                      [ State ]
                    * [ Reply-Message ]
                      [ Origin-State-Id ]
                    * [ NAS-Session-Key ]
                    * [ AVP ]
                    * [ Proxy-Info ]
                    * [ Route-Record ]
```

The Result-Code AVP within the AA-Answer message may be used to indicate authentication success/failure. A value of 4001 denotes that authentication was rejected by the DIAMETER server, while a value of 2001 denotes authentication success.

3.3 Suitability of DIAMETER NASREQ Application

Section 2.3 of [9] discusses extensibility of the DIAMETER protocol, and suggestions for protocol designers on how/when DIAMETER may be extended to fit emerging needs. Some key aspects of this discussion are:

- A new DIAMETER application should only be created as a last resort, if major changes are needed to support the new required functionality.
- When an existing DIAMETER application can be used to handle the new functionality, a new AVP may be created only if an existing AVP cannot carry the information.
- New AVPs within an existing DIAMETER application (say NASREQ) may be created for carrying service-specific information when the DIAMETER application is suitable for the new functionality.

Based on this, the NASREQ DIAMETER application was found suitable as a AAA framework for Basic/Digest authentication. Specifically, the AA-Request and AA-Answer commands are used for the purpose. Three new AVPs (for which AVP codes need to be assigned) are being proposed:

- "Resource" AVP: The AVP is of type OctetString and is used to convey a resource. In this document, it is used by a DIAMETER client to convey to the DIAMETER server the resource whose access needs authorization.
- "Challenge" AVP: The AVP is of type OctetString and is used to convey a challenge. In this document, it is used by a DIAMETER server to convey a challenge to the DIAMETER client.
- "Response" AVP: The AVP is of type OctetString and is used to

convey a response. In this document, it is used by a DIAMETER client to convey a response to the DIAMETER server.

It may be noted that existing NASREQ application AVPs could potentially be used to carry the information being carried within the new AVPs. For instance, the "User-Name" AVP may be used in place of "Resource", the "Reply-Message" AVP may be used in place of "Challenge", and the "CHAP-Challenge" AVP may be used in place of "Response". Since the service-specific information carried within these existing AVPs is different from that needed for our purposes, the creation of new AVPs may be preferred.

It may also be noted that when EAP is used within the "challenge" as proposed within [5], NASREQ application still finds applicability. In this case, the Diameter-EAP-Request and Diameter-EAP-Answer commands are used. However, this is not discussed any further within this document.

4 Use of DIAMETER with Basic/Digest Authentication

4.1 Mapping Overview

In order to achieve the use of a DIAMETER backend framework for a protocol using Basic/Digest authentication, the following mapping is needed:

1) Protocol REQUEST message with no Authorization/Proxy-Authorization header needs to be mapped to AA-Request message
2) AA-Answer message with Result-Code=4001 has to be mapped to 401/407 Response's WWW-Authenticate/Proxy-Authenticate header
3) Protocol REQUEST message with Authorization/Proxy-Authorization header containing Basic/Digest authentication parameters has to be mapped to AA-Request message
4) AA-Answer with Result-Code=2001 has to be mapped to 200 OK Response

For Item 1, we need to construct an AA-Request message from a protocol REQUEST message with no Authorization/Proxy-Authorization header. The Origin-Host and Origin-Realm AVPs have values based on the hostname and domain-name of the DIAMETER client (entity B), and are independent of the protocol REQUEST message. The Destination-Realm AVP is instantiated based either on the Request-Line or on headers such as the From header in the protocol REQUEST message. The Resource AVP carries the resource whose access needs authorization.

For Item 2, the AA-Answer message is first constructed by the

DIAMETER server (entity C). The Origin-Host and Origin-Realm AVPs in the AA-Answer message have values based on the hostname and domain-name of the DIAMETER server (entity C). The Destination-Host AVP in the AA-Answer message has a value identical to the Origin-Host AVP in the AA-Request message. The Challenge AVP is used to contain the "challenge" for Basic or Digest authentication (see Sections 2.1, 2.2), encoded in UTF-8 format. Given the AA-Answer message with Result-Code=4001, we need to construct a 401/407 message. The "challenge" in the Challenge AVP is used for the challenge in the WWW-Authenticate/Proxy-Authenticate header in the 401/407 message.

For Item 3, the Protocol REQUEST message is first constructed by Entity A. Based on the "challenge" in the WWW-Authenticate/Proxy-Authenticate header of the 401/407 message, the "credentials" is computed by A and inserted into the Authorization/Proxy-Authorization header of the Protocol REQUEST message (see Sections 2.1, 2.2). This message needs to be mapped to an AA-Request message. For the case of Basic/Digest authentication, the "credentials" in the WWW-Authenticate/Proxy-Authenticate header is transparently included within the Response AVP of the AA-Request message. The Resource AVP is also included similar to Item 1.

For Item 4, the AA-Answer message with Result-Code AVP of value 2001 is mapped into a 200 OK Response message.

When SIP is used, the resource whose access is being authorized (and which is carried in the Resource AVP), has the following format:

```
resource = [ userinfo "@" ] hostport
hostport = host [ ":" port ]
```

Specific details of the fields may be obtained from [1].

When HTTP is used, the resource whose access is being authorized (and which is carried in the Resource AVP), has the following format:

```
resource = absoluteURI
```

Specific details of absoluteURI may be obtained from [2].

In addition, each AA-Request and AA-Answer message includes:

- the Auth-Application-Id AVP with a value of 1 indicating NASREQ.
- the Service-Type AVP with a value of 8 indicating "Authenticate Only" [11].

4.2 Basic/Digest Authentication for SIP

In the following, the Basic/Digest authentication schemes are used within the SIP protocol, while DIAMETER is used in the backend.

Figure 2 depicts a typical first phase of authentication with SIP, when a UAC communicates with a UAS. Since no Authorization header is included within the SIP INVITE Request and access to the resource identified by the Request-URI field in the SIP INVITE Request needs authorization, the DIAMETER AA-Answer message includes a Result-Code AVP of value 4001. Based on policy, a decision of the authentication mechanism - Basic or Digest - is made at the DIAMETER server and conveyed to UAS in the AA-Answer message. The AA-Answer message translates to a 401 Unauthorized message from the UAS to UAC.

```
         +----+ SIP INVITE            +----+ DIAMETER       +----+
         |    | no Authorization hdr  |    | AA-Request     |    |
         |    |---------------------->|    |--------------->|    |
         |UAC |                       |UAS |                | BS |
         |    |<----------------------|    |<---------------|    |
         |    |     401               |    | DIAMETER       |    |
         +----+ Unauthorized          +----+ AA-Answer      +----+
                                             Result-Code=4001
```

Figure 2: Typical first phase of Authentication for SIP

Figure 3 depicts a typical second phase of authentication with SIP when a UAC communicates with a UAS. Here, an appropriate Authorization header has been included within the SIP INVITE Request. The information in the Authorization header is conveyed within he DIAMETER AA-Request message to the DIAMETER server. Upon successful authentication, an AA-Answer message with Result-Code AVP set to 2001 is returned, which translates to a 200 OK response from the UAS to UAC.

```
         +----+    SIP INVITE          +----+ DIAMETER       +----+
         |    | Authorization hdr      |    | AA-Request     |    |
         |    |----------------------->|    |--------------->|    |
         |UAC |                        |UAS |                | BS |
         |    |<-----------------------|    |<---------------|    |
         |    |      200 OK            |    | DIAMETER       |    |
         +----+                        +----+ AA-Answer      +----+
                                              Result-Code=2001
```

Figure 3: Typical second phase of Authentication for SIP

The case of a SIP Proxy Server authenticating a UAC is similar, with a couple of differences. A 407 Response containing a Proxy-Authenticate header is returned in the first phase. The new SIP INVITE Request in the second phase contains a Proxy-Authorization header.

4.2.1 Illustrating Basic Authentication for SIP

Figure 4 illustrates the mapping from a SIP INVITE message (containing no Authorization header) to a DIAMETER AA-Request message for a typical first phase. The resource whose access needs to be authorized is obtained from the Request-URI field, which has a value "sip:watson@boston.nokia.com:5060;transport=TCP". The userinfo, host and port are included in the Resource AVP, which then has a value of "watson@boston.nokia.com:5060". The Origin-Host AVP has a value of boston.nokia.com, and the Origin-Realm AVP has a value of nokia.com. Since the authentication info needed for resource authorization is accessible to a DIAMETER server at bell-tel.com domain, so the Destination-Realm is bell-tel.com.

```
SIP INVITE Message:
   INVITE sip:watson@boston.nokia.com:5060;transport=TCP SIP/2.0
   From: A. Bell <sip:a.g.bell@bell-tel.com>;tag=3pcc
   To: T. Watson <sip:watson@nokia.com>

DIAMETER AA-Request Message:
    <Diameter Header: 265, REQUEST >
        < Session-Id >={263,boston.nokia.com;13579;12}
        { Auth-Application-Id }={258,1}
        { Origin-Host }={264, boston.nokia.com}
        { Origin-Realm }={296, nokia.com}
        { Destination-Realm }={283, bell-tel.com}
        [ Resource ]=[TBD, watson@boston.nokia.com:5060]
        { Service-Type }={6,8}
```

Figure 4: SIP INVITE (with No Authorization Header) to DIAMETER AA-Request mapping

Figure 5 illustrates the mapping from a DIAMETER AA-Answer message to a SIP 401 message. As seen, the Challenge AVP is used to convey the "challenge", which in this case is 'Basic realm="BUSINESS"'.

```
DIAMETER AA-Answer Message:
     < Diameter Header: 265>
         < Session-Id >={263, boston.nokia.com;13579;12}
         { Auth-Application-Id }={258,1}
         { Result-Code }={268, 4001}
         { Origin-Host }={264, aaa.bel-tel.com}
         { Origin-Realm }={296, bell-tel.com}
         { Service-Type }={6,8}
         { Destination-Host }={293, boston.nokia.com}
        *[ Challenge ]=[TBD, Basic realm="BUSINESS"]

SIP 401 Response Message:
      SIP/2.0 401 Unauthorized
      WWW-Authenticate: Basic realm="BUSINESS"
      From: A. Bell <sip:a.g.bell@bell-tel.com>;tag=3pcc
      To: T. Watson <sip:watson@nokia.com>
```

Figure 5: DIAMETER AA-Answer (with Basic) to SIP 401 Response mapping

Figure 6 illustrates the mapping from a SIP INVITE message (with an

Authorization header) to a DIAMETER AA-Request message for a typical second phase of Basic authentication. The Authorization header contains the credentials " Basic YS5nLmJIbGw6YmVsbHNQYXNzd29yZA==", where "YS5nLmJIbGw6YmVsbHNQYXNzd29yZA==" denotes the Base64 encoding of "a.g.bell:bellsPassword". Here, the user-name is assumed to be "a.g.bell" and the password is assumed to be "bellsPassword". The newly created Response AVP carries the "credentials", which in this case would be " Basic YS5nLmJIbGw6YmVsbHNQYXNzd29yZA==". The Resource AVP contains a value identical to that in Figure 4.

```
SIP INVITE Message:
   INVITE sip:watson@nokia.com:5060;transport=TCP SIP/2.0
   Authorization: Basic YS5nLmJIbGw6YmVsbHNQYXNzd29yZA==
   From: A. Bell <sip:a.g.bell@bell-tel.com>;tag=3pcc
   To: T. Watson <sip:watson@nokia.com>

DIAMETER AA-Request Message:
   <Diameter Header: 265, REQUEST >
   < Session-Id >={263, boston.nokia.com;13579;12}
   { Auth-Application-Id }={258,1}
   { Origin-Host }={264, boston.nokia.com}
   { Origin-Realm }={296, nokia.com}
   { Destination-Realm }={283, bell-tel.com}
   { Service-Type }={6,8}
   [ Resource ]=[TBD, watson@boston.nokia.com:5060]
   [ Response ]=[TBD, Basic YS5nLmJIbGw6YmVsbHNQYXNzd29yZA==]
```

Figure 6: SIP INVITE (with Basic Authorization header) to DIAMETER AA-REQUEST Mapping

Figure 7 depicts the DIAMETER AA-Answer to SIP 200 OK Response mapping.

```
            DIAMETER AA-Answer Message:
                < Diameter Header: 265>
                   < Session-Id >=<263, boston.nokia.com;13579;12>
                   { Auth-Application-Id }={258,1}
                   { Result-Code }={268, 2001}
                   { Origin-Host }={264, aaa.bell-tel.com}
                   { Origin-Realm }={296, bell-tel.com}
                   { Service-Type }={6,8}
                   { Destination-Host }={293, boston.nokia.com}


            SIP 200 Response Message:
                SIP/2.0 200 OK
                From: A. Bell <sip:a.g.bell@bell-tel.com>;tag=3pcc
                To: T. Watson <sip:watson@nokia.com>
```

Figure 7: DIAMETER AA-ANSWER (Result-Code=2001) to SIP 200 OK Response Mapping

4.2.2 Digest Authentication for SIP

In the case of Digest authentication, the mapping of the first SIP INVITE message (containing no Authorization header) to a DIAMETER AA-Request message is identical to the case of Basic authentication (see Figure 4).

Figure 8 illustrates the mapping from a DIAMETER AA-Answer message indicating the need for Digest authentication to a SIP 401 message. As seen, the Challenge AVP is used to convey the "challenge", which in this case is denoted by the generic value of "Digest digest-challenge". The "digest-challenge" includes the nonce, realm and opaque parameters, among others. For instance, values for nonce, realm and opaque in the "digest-challenge" may be: realm="Business", nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093", opaque="5ccc069c403ebaf9f0171e9517f40e41". The WWW-Authenticate header within the 401 message transparently carries the "challenge".

```
            DIAMETER AA-Answer Message:
                 < Diameter Header: 265>
                     < Session-Id >={263, boston.nokia.com;13579;12}
                     { Auth-Application-Id }={258,1}
                     { Result-Code }={268, 4001}
                     { Origin-Host }={264, aaa.bel-tel.com}
                     { Origin-Realm }={296, bell-tel.com}
                     { Service-Type }={6,8}
                     { Destination-Host }={293, boston.nokia.com}
                    *[ Challenge ]=[TBD, Digest digest-challenge]

            SIP 401 Response Message:
                  SIP/2.0 401 Unauthorized
                  WWW-Authenticate: Digest digest-challenge
                  From: A. Bell <sip:a.g.bell@bell-tel.com>;tag=3pcc
                  To: T. Watson <sip:watson@nokia.com>
```

Figure 8: DIAMETER AA-Answer (with Digest) to SIP 401 Response mapping

Figure 9 illustrates the mapping from a SIP INVITE message (with an Authorization header) to a DIAMETER AA-Request message for a typical second phase of Digest authentication. The Authorization header carries the "credentials" which is generically denoted here as "Digest digest-response". The "digest-response" could include fields such as:

- username="a.g.bell"
- realm="Business"
- nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093"
- response="6629fae49393a05397450978507c4ef1", which is the MD5 hash of the password and a few other parameters
- opaque="5ccc069c403ebaf9f0171e9517f40e41"

In the AA-Request message, the Response AVP is used to carry the "credentials".

```
            SIP INVITE Message:
                INVITE sip:watson@nokia.com:5060;transport=TCP SIP/2.0
                Authorization: Digest digest-response
                From: A. Bell <sip:a.g.bell@bell-tel.com>;tag=3pcc
                To: T. Watson <sip:watson@nokia.com>

            DIAMETER AA-Request Message:
                <Diameter Header: 265, REQUEST >
                    < Session-Id >={263, boston.nokia.com;13579;12}
                    { Auth-Application-Id }={258,1}
                    { Origin-Host }={264, boston.nokia.com}
                    { Origin-Realm }={296, nokia.com}
                    { Destination-Realm }={283, bell-tel.com}
                    { Service-Type }={6,8}
                    [ Resource ]=[TBD, watson@boston.nokia.com:5060]
                    [ Response ]=[TBD, Digest digest-response]
```

Figure 9: SIP INVITE (with Digest Authorization header) to DIAMETER AA-REQUEST Mapping

The DIAMETER AA-Answer (with Result-Code=2001) to SIP 200 OK Response mapping is identical to that of Basic authentication (see Figure 7).

4.2 Basic/Digest Authentication for HTTP

In the following, the use of DIAMETER with HTTP under Basic and Digest Authentication schemes has been described. Similar to the case described in SIP, Figures 10 and 11 illustrate typical first and second phases of authentication for HTTP, respectively.

```
         +-------+ HTTP GET               +-------+ DIAMETER       +----+
         |       | no Authorization hdr   |       | AA-Request     |    |
         |HTTP   |----------------------->|HTTP   |--------------->|    |
         |Client|                         |Server|                 | BS |
         |       |<-----------------------|       |<---------------|    |
         |       |     401                |       | DIAMETER       |    |
         +-------+ Unauthorized           +-------+ AA-Answer      +----+
                                                 Result-Code=4001
```

Figure 10: Typical first phase of Authentication for HTTP

```
+------+ HTTP GET              +------+ DIAMETER       +-----+
|      | Authorization hdr     |      | AA-Request     |     |
|HTTP  |----------------------->|HTTP  |--------------->|     |
|Client|                       |Server|                | BS  |
|      |<----------------------|      |<---------------|     |
|      |     200 OK            |      | DIAMETER       |     |
+------+                       +------+ AA-Answer      +-----+
                                       Result-Code=2001
```

Figure 11: Typical second phase of Authentication for HTTP

4.2.1 Basic Authentication for HTTP

Figure 12 illustrates the mapping from a HTTP GET message (with no Authorization header) to a DIAMETER AA-Request message for a typical first phase. Access to the resource indicated by the URL "www.nokia.com/Boston/index.html" needs to be authorized. Since the authentication info needed for resource authorization is accessible to a DIAMETER server at nokia.com domain, so the Destination-Realm is nokia.com. The From header in the HTTP GET Request is optional, and even if present, typically does not affect construction of the AA-Request message. It may be noted that the Destination-Realm is different for the case in SIP (Section 4.1.1), since the realms that contain the authentication information (needed for resource authorization) are different in the two cases.

```
HTTP GET Message:
    GET www.nokia.com/Boston/index.html HTTP/1.1
    From: a.g.bell@bell-tel.com

DIAMETER AA-Request Message:
     <Diameter Header: 265, REQUEST >
         < Session-Id >={263,boston.nokia.com;13579;12}
         { Auth-Application-Id }={258,1}
         { Origin-Host }={264, boston.nokia.com}
         { Origin-Realm }={296, nokia.com}
         { Destination-Realm }={283, nokia.com}
         [ Resource ]=[TBD, www.nokia.com/Boston/index.html]
         { Service-Type }={6,8}
```

Figure 12: HTTP GET (no Authorization header) to DIAMETER AA-Request mapping

Figure 13 illustrates a DIAMETER AA-Answer message (indicating the need for Basic authentication) and its mapping to a SIP 401 message.

```
         DIAMETER AA-Answer Message:
              < Diameter Header: 265>
                  < Session-Id >={263, boston.nokia.com;13579;12}
                  { Auth-Application-Id }={258,1}
                  { Result-Code }={268, 4001}
                  { Origin-Host }={264, aaa.nokia.com}
                  { Origin-Realm }={296, nokia.com}
                  { Service-Type }={6,8}
                  { Destination-Host }={293, boston.nokia.com}
                 *[ Challenge ]=[TBD, Basic Realm="BUSINESS"]

         HTTP 401 Response Message:
               HTTP/1.1 401 Unauthorized
               WWW-Authenticate: Basic realm="BUSINESS"
```

Figure 13: DIAMETER AA-Answer (with Basic) to HTTP 401 Response mapping

Figure 14 illustrates the mapping from a HTTP GET message (with Basic Authorization header) to a DIAMETER AA-Request message for a typical second phase of Basic authentication.

```
  HTTP GET Message:
     GET www.nokia.com/Boston/index.html HTTP/1.1
     Authorization: Basic YS5nLmJIbGw6YmVsbHNQYXNzd29yZA==
     From: a.g.bell@bell-tel.com

  DIAMETER AA-Request Message:
     <Diameter Header: 265, REQUEST >
         < Session-Id >={263, boston.nokia.com;13579;12}
         { Auth-Application-Id }={258,1}
         { Origin-Host }={264, boston.nokia.com}
         { Origin-Realm }={296, nokia.com}
         { Destination-Realm }={283, nokia.com}
         { Service-Type }={6,8}
         [ Resource ]=[TBD, www.nokia.com/Boston/index.html]
         [ Response ]=[TBD, Basic YS5nLmJIbGw6YmVsbHNQYXNzd29yZA==]
```

Figure 14: HTTP GET (with Basic Authorization header) to

DIAMETER AA-REQUEST Mapping

Figure 15 depicts the DIAMETER AA-Answer (with Result-Code=2001) to HTTP 200 OK Response mapping.

```
DIAMETER AA-Answer Message:
    < Diameter Header: 265>
       < Session-Id >=<263, boston.nokia.com;13579;12>
       { Auth-Application-Id }={258,1}
       { Result-Code }={268, 2001}
       { Origin-Host }={264, aaa.nokia.com}
       { Origin-Realm }={296, nokia.com}
       { Service-Type }={6,8}
       { Destination-Host }={293, boston.nokia.com}


HTTP 200 Response Message:
    HTTP/1.1 200 OK
```

Figure 15: DIAMETER AA-ANSWER (with Result-Code=2001) to HTTP 200 OK Response Mapping

4.2.2 Digest Authentication for HTTP

In the case of Digest authentication, the mapping of the first HTTP GET message (containing no Authorization header) to a DIAMETER AA-Request message is identical to the case of Basic authentication (see Figure 12).

Figure 16 illustrates the DIAMETER AA-Answer to HTTP 401 response mapping for Digest authentication.

```
         DIAMETER AA-Answer Message:
              < Diameter Header: 265>
                  < Session-Id >={263, boston.nokia.com;13579;12}
                  { Auth-Application-Id }={258,1}
                  { Result-Code }={268, 4001}
                  { Origin-Host }={264, aaa.nokia.com}
                  { Origin-Realm }={296, nokia.com}
                  { Service-Type }={6,8}
                  { Destination-Host }={293, boston.nokia.com}
                 *[ Challenge ]=[TBD, Digest digest-challenge]

         HTTP 401 Response Message:
               HTTP/1.1 401 Unauthorized
               WWW-Authenticate: Digest digest-challenge
```

Figure 16: DIAMETER AA-Answer to HTTP 401 Response mapping for Digest

Figure 17 illustrates the typical second phase of Digest authentication with HTTP, which includes an Authorization header in the HTTP GET message.

```
         HTTP GET Message:
             GET www.nokia.com/Boston/index.html HTTP/1.1
             Authorization: Digest digest-response
             From: a.g.bell@bell-tel.com

         DIAMETER AA-Request Message:
             <Diameter Header: 265, REQUEST >
                 < Session-Id >={263, boston.nokia.com;13579;12}
                 { Auth-Application-Id }={258,1}
                 { Origin-Host }={264, boston.nokia.com}
                 { Origin-Realm }={296, nokia.com}
                 { Destination-Realm }={283, nokia.com}
                 { Service-Type }={6,8}
                 [ Resource ]=[TBD, www.nokia.com/Boston/index.html]
                 [ Response ]=[TBD, Digest digest-response]
```

Figure 17: HTTP GET (with Digest Authorization header) to DIAMETER AA-REQUEST Mapping

The DIAMETER AA-Answer (with Result-Code=2001) to HTTP 200 OK Response mapping for Digest authentication is identical to that for Basic authentication (see Figure 15).

References

[1] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP: Session Initiation Protocol", draft-ietf-sip-rfc2543bis-03.txt, IETF work in progress, May 2001.

[2] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[3] R. Stewart, Q. Xie, "Aggregate Server Access Protocol (ASAP)", draft-ietf-rserpool-asap-00.txt, IETF work in progress, June 2001.

[4] Q. Xie, R. Stewart, "Endpoint Name Resolution Protocol (ENRP)", draft-ietf-rserpool-enrf-00.txt, IETF work in progress, June 2001.

[5] J. Arkko, V. Torvinen, A. Niemi, "HTTP Authentication with EAP", draft-http-eap-basic-04.txt, IETF work in progress, June 2001.

[6] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[7] N. Freed, N. Borenstein. "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[8] P. Calhoun, G. Zorn, P. Pan, "Diameter Framework Document", draft-calhoun-diameter-framework-09.txt, IETF work in progress, Febrary 2001.

[9] P. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A. Rubens, "Diameter Base Protocol", draft-ietf-aaa-diameter-05.txt, IETF work in progress, June 2001.

[10] P. Calhoun, W. Bulley, A. Rubens, J. Haag, "Diameter NASREQ Extension", draft-ietf-aaa-diameter-nasreq-06.txt, IETF work in progress, June 2001.

[11] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

Acknowledgements

We would like acknowledge Jaakko Rajaniemi and Patrik Flykt (Nokia) for providing comments.

Authors's Addresses

Bindignavile Srinivas
Tat Chan
Senthil Sengodan
Jose Costa-Requena

Nokia Research Center
5 **Wayside Road**
Burlington, MA 01803
USA

{bindignavile.srinivas,tat.chan,senthil.sengodan,jose.costa-requena}
@nokia.com