HTTPAuth Working Group
Internet-Draft
Obsoletes: 2617 (if approved)
Intended Status: Standards Track
Expires: July 5, 2014

R. Shekh-Yusef, Ed.
D. Ahrens
Avaya
S. Bremer
Netzkonform

January 1, 2014

HTTP Digest Access Authentication
draft-ietf-httpauth-digest-01.txt

Abstract

HTTP provides a simple challenge-response authentication mechanism that may be used by a server to challenge a client request and by a client to provide authentication information. This document defines the HTTP Digest Authentication scheme that may be used with the authentication mechanism.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Table of Contents

1 Introduction

HTTP provides a simple challenge-response authentication mechanism that MAY be used by a server to challenge a client request and by a client to provide authentication information. It uses an extensible, case-insensitive token to identify the authentication scheme, followed by a comma-separated list of attribute-value pairs which carry the parameters necessary for achieving authentication via that scheme.

```
auth-scheme    = token
auth-param     = token "=" ( token | quoted-string )
```

The 401 (Unauthorized) response message is used by an origin server to challenge the authorization of a user agent. This response MUST include a WWW-Authenticate header field containing at least one challenge applicable to the requested resource. The 407 (Proxy Authentication Required) response message is used by a proxy to challenge the authorization of a client and MUST include a Proxy-Authenticate header field containing at least one challenge applicable to the proxy for the requested resource.

```
challenge   = auth-scheme 1*SP 1#auth-param
```

Note: User agents will need to take special care in parsing the WWW-Authenticate or Proxy-Authenticate header field value if it contains more than one challenge, or if more than one WWW-Authenticate header field is provided, since the contents of a challenge may itself contain a comma-separated list of authentication parameters.

The authentication parameter realm is defined for all authentication schemes:

```
realm       = "realm" "=" realm-value
realm-value = quoted-string
```

The realm directive (case-insensitive) is required for all authentication schemes that issue a challenge. The realm value (case-sensitive), in combination with the canonical root URL (the absoluteURI for the server whose abs_path is empty; see section 5.1.2 of [RFC2616]) of the server being accessed, defines the protection space. These realms allow the protected resources on a server to be partitioned into a set of protection spaces, each with its own authentication scheme and/or authorization database. The realm value is a string, generally assigned by the origin server, which may have additional semantics specific to the authentication scheme. Note that there may be multiple challenges with the same auth-scheme but different realms.

A user agent that wishes to authenticate itself with an origin server--usually, but not necessarily, after receiving a 401 (Unauthorized)--MAY do so by including an Authorization header field with the request. A client that wishes to authenticate itself with a proxy--usually, but not necessarily, after receiving a 407 (Proxy Authentication Required)--MAY do so by including a Proxy-Authorization header field with the request. Both the Authorization field value and the Proxy-Authorization field value consist of credentials containing the authentication information of the client for the realm of the resource being requested. The user agent MUST choose to use one of the challenges with the strongest auth-scheme it understands and request credentials from the user based upon that challenge.

credentials = auth-scheme #auth-param

Note that many browsers will only recognize Basic and will require that it be the first auth-scheme presented. Servers should only include Basic if it is minimally acceptable.

The protection space determines the domain over which credentials can be automatically applied. If a prior request has been authorized, the same credentials MAY be reused for all other requests within that protection space for a period of time determined by the authentication scheme, parameters, and/or user preference. Unless otherwise defined by the authentication scheme, a single protection space cannot extend outside the scope of its server.

If the origin server does not wish to accept the credentials sent with a request, it SHOULD return a 401 (Unauthorized) response. The response MUST include a WWW-Authenticate header field containing at least one (possibly new) challenge applicable to the requested resource. If a proxy does not accept the credentials sent with a request, it SHOULD return a 407 (Proxy Authentication Required). The response MUST include a Proxy-Authenticate header field containing a (possibly new) challenge applicable to the proxy for the requested resource.

The HTTP protocol does not restrict applications to this simple challenge-response mechanism for access authentication. Additional mechanisms MAY be used, such as encryption at the transport level or via message encapsulation, and with additional header fields specifying authentication information. However, these additional mechanisms are not defined by this specification.

Proxies MUST be completely transparent regarding user agent authentication by origin servers. That is, they must forward the WWW-Authenticate and Authorization headers untouched, and follow the

rules found in section 14.8 of [RFC2616]. Both the Proxy-Authenticate and the Proxy-Authorization header fields are hop-by-hop headers (see section 13.5.1 of [RFC2616]).

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].

2 Syntax Convention

In the interest of clarity and readability, the extended parameters or the headers and parameters in the examples in this document might be broken into multiple lines. Any line that is indented in this document is a continuation of the preceding line.

3 Digest Access Authentication Scheme

3.1 Overall Operation

The Digest scheme is based on a simple challenge-response paradigm. The Digest scheme challenges using a nonce value. A valid response contains a checksum of the username, the password, the given nonce value, the HTTP method, and the requested URI. In this way, the password is never sent in the clear. The username and password must be prearranged in some fashion not addressed by this document.

3.2 Representation of Digest Values

An optional header allows the server to specify the algorithm used to create the checksum or digest. By default the SHA2-256 algorithm is used, with SHA2-512/256 being used as a backup algorithm. To maintain backwards compatibility, the MD5 algorithm is still supported but not recommended.

The size of the digest depends on the algorithm used. The bits in the digest are converted from the most significant to the least significant bit, four bits at a time to the ASCII representation as follows. Each four bits is represented by its familiar hexadecimal notation from the characters 0123456789abcdef, that is binary 0000 is represented by the character '0', 0001 by '1' and so on up to the representation of 1111 as 'f'. If the MD5 algorithm is used to calculate the digest, then the digest will be represented as 32 hexadecimal characters, SHA2-256 and SHA2-512/256 by 64 hexadecimal characters.

3.3 The WWW-Authenticate Response Header

If a server receives a request for an access-protected object, and an acceptable Authorization header is not sent, the server responds with a "401 Unauthorized" status code, and a WWW-Authenticate header as per the framework defined above, which for the digest scheme is utilized as follows:

```
challenge         =  "Digest" digest-challenge

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

domain            = "domain" "=" <"> URI ( 1*SP URI ) <">
URI               = absoluteURI | abs_path
nonce             = "nonce" "=" nonce-value
nonce-value       = quoted-string
opaque            = "opaque" "=" quoted-string
stale             = "stale" "=" ( "true" | "false" )
algorithm         = "algorithm" "=" (
                    "MD5" | "MD5-sess" |
                    "SHA2-256" | "SHA2-256-sess" |
                    "SHA2-512-256" | "SHA2-512-256-sess" |
                    token)
qop-options       = "qop" "=" <"> 1#qop-value <">
qop-value         = "auth" | "auth-int" | token
charset           = "charset" "=" ("UTF-8" | token)
userhash          = "userhash" "=" ( "true" | "false" )
```

The meanings of the values of the directives used above are as follows:

realm
: A string to be displayed to users so they know which username and password to use. This string should contain at least the name of the host performing the authentication and might additionally indicate the collection of users who might have access. An example might be "registered_users@gotham.news.com".

domain
: A quoted, space-separated list of URIs, as specified in RFC XURI [7], that define the protection space. If a URI is an abs_path, it is relative to the canonical root URL of the server being accessed. An absoluteURI in this list may refer to a different server than the one being accessed. The client can use this list

to determine the set of URIs for which the same authentication information may be sent: any URI that has a URI in this list as a prefix (after both have been made absolute) may be assumed to be in the same protection space. If this directive is omitted or its value is empty, the client should assume that the protection space consists of all URIs on the responding server.

This directive is not meaningful in Proxy-Authenticate headers, for which the protection space is always the entire proxy; if present it should be ignored.

nonce

A server-specified data string which should be uniquely generated each time a 401 response is made. It is recommended that this string be base64 or hexadecimal data. Specifically, since the string is passed in the header lines as a quoted string, the double-quote character is not allowed.

The contents of the nonce are implementation dependent. The quality of the implementation depends on a good choice. A nonce might, for example, be constructed as the base 64 encoding of

time-stamp H(time-stamp ":" ETag ":" private-key)

where time-stamp is a server-generated time or other non-repeating value, ETag is the value of the HTTP ETag header associated with the requested entity, and private-key is data known only to the server. With a nonce of this form a server would recalculate the hash portion after receiving the client authentication header and reject the request if it did not match the nonce from that header or if the time-stamp value is not recent enough. In this way the server can limit the time of the nonce's validity. The inclusion of the ETag prevents a replay request for an updated version of the resource. (Note: including the IP address of the client in the nonce would appear to offer the server the ability to limit the reuse of the nonce to the same client that originally got it. However, that would break proxy farms, where requests from a single user often go through different proxies in the farm. Also, IP address spoofing is not that hard.)

An implementation might choose not to accept a previously used nonce or a previously used digest, in order to protect against a replay attack. Or, an implementation might choose to use one-time nonces or digests for POST or PUT requests and a time-stamp for GET requests. For more details on the issues involved see section 5 of this document.

The nonce is opaque to the client.

opaque
A string of data, specified by the server, which should be returned by the client unchanged in the Authorization header of subsequent requests with URIs in the same protection space. It is recommended that this string be base64 or hexadecimal data.

stale
A case-insensitive flag, indicating that the previous request from the client was rejected because the nonce value was stale. If stale is TRUE, the client may wish to simply retry the request with a new encrypted response, without reprompting the user for a new username and password. The server should only set stale to TRUE if it receives a request for which the nonce is invalid but with a valid digest for that nonce (indicating that the client knows the correct username/password). If stale is FALSE, or anything other than TRUE, or the stale directive is not present, the username and/or password are invalid, and new values must be obtained.

algorithm
A string indicating a pair of algorithms used to produce the digest and a checksum. If this is not present it is assumed to be "MD5". If the algorithm is not understood, the challenge should be ignored (and a different one used, if there is more than one).

In this document the string obtained by applying the digest algorithm to the data "data" with secret "secret" will be denoted by KD(secret, data), and the string obtained by applying the checksum algorithm to the data "data" will be denoted H(data). The notation unq(X) means the value of the quoted-string X without the surrounding quotes.

For the "MD5" and "MD5-sess" algorithms

H(data) = MD5(data)

For the "SHA2-256" and "SHA2-256-sess" algorithms

H(data) = SHA2-256(data)

For the "SHA2-512-256" and "SHA2-512-256-sess" algorithms

H(data) = SHA2-512-256(data)

and

KD(secret, data) = H(concat(secret, ":", data))

i.e., the digest is the MD5 of the secret concatenated with a colon concatenated with the data. The "MD5-sess" algorithm is intended to allow efficient 3rd party authentication servers; for the difference in usage, see the description in section 3.4.2.

qop-options
: This directive is optional, but is made so only for backward compatibility with RFC 2069 [RFC2069]; it SHOULD be used by all implementations compliant with this version of the Digest scheme. If present, it is a quoted string of one or more tokens indicating the "quality of protection" values supported by the server. The value "auth" indicates authentication; the value "auth-int" indicates authentication with integrity protection; see the descriptions below for calculating the response directive value for the application of this choice. Unrecognized options MUST be ignored.

charset
: This is an optional parameter that could be used by the server to indicate the encoding scheme it supports.

userhash
: This is an optional parameter that could be used by the server to indicate that it supports username hashing.

auth-param
: This directive allows for future extensions. Any unrecognized directive MUST be ignored.

3.4 The Authorization Request Header

The client is expected to retry the request, passing an Authorization header line, which is defined according to the framework above, utilized as follows.

```
credentials      = "Digest" digest-response
digest-response  = 1#( username | realm | nonce | digest-uri |
                   response | [ algorithm ] | [cnonce] |
                   [opaque] | [message-qop] |
                   [nonce-count]  | [charset] | [userhash] |
                   [auth-param] )
username         = "username" "=" username-value
username-value   = quoted-string
digest-uri       = "uri" "=" digest-uri-value
digest-uri-value = request-uri   ; As specified by HTTP/1.1
message-qop      = "qop" "=" qop-value
```

```
        cnonce           = "cnonce" "=" cnonce-value
        cnonce-value     = nonce-value
        nonce-count      = "nc" "=" nc-value
        nc-value         = 8LHEX
        response         = "response" "=" request-digest
        request-digest = <"> digest-size LHEX <">
        digest-size       = "32" | "64"
        LHEX             =  "0" | "1" | "2" | "3" |
                            "4" | "5" | "6" | "7" |
                            "8" | "9" | "a" | "b" |
                            "c" | "d" | "e" | "f"
        charset           = "charset" "=" ("UTF-8" | token)
        userhash          = "userhash" "=" ( "true" | "false" )
```

The values of the opaque and algorithm fields must be those supplied in the WWW-Authenticate response header for the entity being requested.

response
: A string of digest-size hex digits computed as defined below, which proves that the user knows a password

username
: The user's name in the specified realm.

digest-uri
: The URI from Request-URI of the Request-Line; duplicated here because proxies are allowed to change the Request-Line in transit.

qop
: Indicates what "quality of protection" the client has applied to the message. If present, its value MUST be one of the alternatives the server indicated it supports in the WWW-Authenticate header. These values affect the computation of the request-digest. Note that this is a single token, not a quoted list of alternatives as in WWW- Authenticate. This directive is optional in order to preserve backward compatibility with a minimal implementation of RFC 2069 [RFC2069], but SHOULD be used if the server indicated that qop is supported by providing a qop directive in the WWW-Authenticate header field.

cnonce
: This MUST be specified if a qop directive is sent (see above), and MUST NOT be specified if the server did not send a qop directive in the WWW-Authenticate header field. The cnonce-value is an opaque quoted string value provided by the client and used by both client and server to avoid chosen plaintext attacks, to provide mutual authentication, and to provide some message integrity

protection. See the descriptions below of the calculation of the response- digest and request-digest values.

nonce-count
: This MUST be specified if a qop directive is sent (see above), and MUST NOT be specified if the server did not send a qop directive in the WWW-Authenticate header field. The nc-value is the hexadecimal count of the number of requests (including the current request) that the client has sent with the nonce value in this request. For example, in the first request sent in response to a given nonce value, the client sends "nc=00000001". The purpose of this directive is to allow the server to detect request replays by maintaining its own copy of this count - if the same nc-value is seen twice, then the request is a replay. See the description below of the construction of the request-digest value.

charset
: This is an optional parameter that could be used by the client to indicate the encoding scheme it supports.

userhash
: This is an optional parameter that could be used by the client to indicate that it supports username hashing.

auth-param
: This directive allows for future extensions. Any unrecognized directive MUST be ignored.

If a directive or its value is improper, or required directives are missing, the proper response is 400 Bad Request. If the request-digest is invalid, then a login failure should be logged, since repeated login failures from a single client may indicate an attacker attempting to guess passwords.

The definition of request-digest above indicates the encoding for its value. The following definitions show how the value is computed.

3.4.1 Request-Digest

If the "qop" value is "auth" or "auth-int":

```
request-digest  = <"> < KD ( H(A1), unq(nonce-value)
                                    ":" nc-value
                                    ":" unq(cnonce-value)
                                    ":" unq(qop-value)
                                    ":" H(A2)
                            ) <">
```

If the "qop" directive is not present (this construction is for compatibility with RFC 2069):

```
request-digest =
   <"> < KD ( H(A1), unq(nonce-value) ":" H(A2) ) > <">
```

See below for the definitions for A1 and A2.

3.4.2 A1

If the "algorithm" directive's value is "MD5", "SHA2-256", or "SHA2-512-256", then A1 is:

```
A1       = unq(username-value) ":" unq(realm-value) ":" passwd
```

where

```
passwd   = < user's password >
```

If the "algorithm" directive's value is "MD5-sess", "SHA2-256-sess", or "SHA2-512-256-sess", then A1 is calculated only once - on the first request by the client following receipt of a WWW-Authenticate challenge from the server. It uses the server nonce from that challenge, and the first client nonce value to construct A1 as follows:

```
A1       = H( unq(username-value) ":" unq(realm-value)
              ":" passwd )
              ":" unq(nonce-value) ":" unq(cnonce-value)
```

This creates a 'session key' for the authentication of subsequent requests and responses which is different for each "authentication session", thus limiting the amount of material hashed with any one key. (Note: see further discussion of the authentication session in section 3.6.) Because the server need only use the hash of the user credentials in order to create the A1 value, this construction could be used in conjunction with a third party authentication service so that the web server would not need the actual password value. The specification of such a protocol is beyond the scope of this specification.

3.4.3 A2

If the "qop" directive's value is "auth" or is unspecified, then A2 is:

```
A2       = Method ":" digest-uri-value
```

If the "qop" value is "auth-int", then A2 is:

```
A2       = Method ":" digest-uri-value ":" H(entity-body)
```

3.4.4 Username Hashing

To protect the transport of the username from the client to the server, the server SHOULD set the "userhash" parameter with the value of "true" in the WWW-Authentication header.

If the client supports the "userhash" parameter, and the "userhash" parameter value in the WWW-Authentication header is set to "true", then the client SHOULD calculate a hash of the username after any other hash calculation and include the "userhash" parameter with the value of "true" in the Authorization Request Header. If the client does not provide the "username" as a hash value or the "userhash" parameter with the value of "true", the server MAY reject the request.

The server may change the nonce value, so the client should be ready to recalculate the hashed username.

The following is the operation that the client will take to hash the username:

```
username = H( H( username ":" realm ) ":" nonce)
```

3.4.5 Directive Values and Quoted-String

Note that the value of many of the directives, such as "username-value", are defined as a "quoted-string". However, the "unq" notation indicates that surrounding quotation marks are removed in forming the string A1. Thus if the Authorization header includes the fields

```
username="Mufasa", realm=myhost@testrealm.com
```

and the user Mufasa has password "Circle Of Life" then H(A1) would be H(Mufasa:myhost@testrealm.com:Circle Of Life) with no quotation marks in the digested string.

No white space is allowed in any of the strings to which the digest function H() is applied unless that white space exists in the quoted strings or entity body whose contents make up the string to be digested. For example, the string A1 illustrated above must be

Mufasa:myhost@testrealm.com:Circle Of Life

with no white space on either side of the colons, but with the white space between the words used in the password value. Likewise, the other strings digested by H() must not have white space on either side of the colons which delimit their fields unless that white space was in the quoted strings or entity body being digested.

Also note that if integrity protection is applied (qop=auth-int), the H(entity-body) is the hash of the entity body, not the message body - it is computed before any transfer encoding is applied by the sender and after it has been removed by the recipient. Note that this includes multipart boundaries and embedded headers in each part of any multipart content-type.

3.4.6 Various Considerations

The "Method" value is the HTTP request method as specified in section 5.1.1 of [RFC2616]. The "request-uri" value is the Request-URI from the request line as specified in section 5.1.2 of [RFC2616]. This may be "*", an "absoluteURL" or an "abs_path" as specified in section 5.1.2 of [RFC2616], but it MUST agree with the Request-URI. In particular, it MUST be an "absoluteURL" if the Request-URI is an "absoluteURL". The "cnonce-value" is an optional client-chosen value whose purpose is to foil chosen plaintext attacks.

The authenticating server must assure that the resource designated by the "uri" directive is the same as the resource specified in the Request-Line; if they are not, the server SHOULD return a 400 Bad Request error. (Since this may be a symptom of an attack, server implementers may want to consider logging such errors.) The purpose of duplicating information from the request URL in this field is to deal with the possibility that an intermediate proxy may alter the client's Request-Line. This altered (but presumably semantically equivalent) request would not result in the same digest as that calculated by the client.

Implementers should be aware of how authenticated transactions interact with shared caches. The HTTP/1.1 protocol specifies that when a shared cache (see section 13.7 of [RFC2616]) has received a request containing an Authorization header and a response from relaying that request, it MUST NOT return that response as a reply to

any other request, unless one of two Cache-Control (see section 14.9 of [RFC2616]) directives was present in the response. If the original response included the "must-revalidate" Cache-Control directive, the cache MAY use the entity of that response in replying to a subsequent request, but MUST first revalidate it with the origin server, using the request headers from the new request to allow the origin server to authenticate the new request. Alternatively, if the original response included the "public" Cache-Control directive, the response entity MAY be returned in reply to any subsequent request.

3.5 The Authentication-Info Header

The Authentication-Info header is used by the server to communicate some information regarding the successful authentication in the response.

```
AuthenticationInfo = "Authentication-Info" ":" auth-info
auth-info          = 1#(nextnonce | [ message-qop ]
                        | [ response-auth ] | [ cnonce ]
                        | [nonce-count] )
nextnonce          = "nextnonce" "=" nonce-value
response-auth      = "rspauth" "=" response-digest
response-digest    = <"> digest-size LHEX <">
digest-size        = "32" | "64"
```

The value of the nextnonce directive is the nonce the server wishes the client to use for a future authentication response. The server may send the Authentication-Info header with a nextnonce field as a means of implementing one-time or otherwise changing nonces. If the nextnonce field is present the client SHOULD use it when constructing the Authorization header for its next request. Failure of the client to do so may result in a request to re-authenticate from the server with the "stale=TRUE".

> Server implementations should carefully consider the performance implications of the use of this mechanism; pipelined requests will not be possible if every response includes a nextnonce directive that must be used on the next request received by the server. Consideration should be given to the performance vs. security tradeoffs of allowing an old nonce value to be used for a limited time to permit request pipelining. Use of the nonce-count can retain most of the security advantages of a new server nonce without the deleterious affects on pipelining.

message-qop
: Indicates the "quality of protection" options applied to the response by the server. The value "auth" indicates authentication; the value "auth-int" indicates authentication with

integrity protection. The server SHOULD use the same value for the message- qop directive in the response as was sent by the client in the corresponding request.

The optional response digest in the "response-auth" directive supports mutual authentication -- the server proves that it knows the user's secret, and with qop=auth-int also provides limited integrity protection of the response. The "response-digest" value is calculated as for the "request-digest" in the Authorization header, except that if "qop=auth" or is not specified in the Authorization header for the request, A2 is

```
A2       = ":" digest-uri-value
```

and if "qop=auth-int", then A2 is

```
A2       = ":" digest-uri-value ":" H(entity-body)
```

where "digest-uri-value" is the value of the "uri" directive on the Authorization header in the request. The "cnonce-value" and "nc-value" MUST be the ones for the client request to which this message is the response. The "response-auth", "cnonce", and "nonce-count" directives MUST BE present if "qop=auth" or "qop=auth-int" is specified.

The Authentication-Info header is allowed in the trailer of an HTTP message transferred via chunked transfer-coding.

3.6 Digest Operation

Upon receiving the Authorization header, the server may check its validity by looking up the password that corresponds to the submitted username. Then, the server must perform the same digest operation (e.g., MD5) performed by the client, and compare the result to the given request-digest value.

Note that the HTTP server does not actually need to know the user's cleartext password. As long as H(A1) is available to the server, the validity of an Authorization header may be verified.

The client response to a WWW-Authenticate challenge for a protection space starts an authentication session with that protection space. The authentication session lasts until the client receives another WWW-Authenticate challenge from any server in the protection space. A client should remember the username, password, nonce, nonce count and opaque values associated with an authentication session to use to construct the Authorization header in future requests within that protection space. The Authorization header may be included

preemptively; doing so improves server efficiency and avoids extra round trips for authentication challenges. The server may choose to accept the old Authorization header information, even though the nonce value included might not be fresh. Alternatively, the server may return a 401 response with a new nonce value, causing the client to retry the request; by specifying stale=TRUE with this response, the server tells the client to retry with the new nonce, but without prompting for a new username and password.

Because the client is required to return the value of the opaque directive given to it by the server for the duration of a session, the opaque data may be used to transport authentication session state information. (Note that any such use can also be accomplished more easily and safely by including the state in the nonce.) For example, a server could be responsible for authenticating content that actually sits on another server. It would achieve this by having the first 401 response include a domain directive whose value includes a URI on the second server, and an opaque directive whose value contains the state information. The client will retry the request, at which time the server might respond with a 301/302 redirection, pointing to the URI on the second server. The client will follow the redirection, and pass an Authorization header , including the <opaque> data.

As with the basic scheme, proxies must be completely transparent in the Digest access authentication scheme. That is, they must forward the WWW-Authenticate, Authentication-Info and Authorization headers untouched. If a proxy wants to authenticate a client before a request is forwarded to the server, it can be done using the Proxy-Authenticate and Proxy-Authorization headers described in section 3.6 below.

3.7 Security Protocol Negotiation

It is useful for a server to be able to know which security schemes a client is capable of handling.

It is possible that a server may want to require Digest as its authentication method, even if the server does not know that the client supports it. A client is encouraged to fail gracefully if the server specifies only authentication schemes it cannot handle.

When a server receives a request to access a resource, the server might challenge the client by responding with "401 Unauthorized" status code, and include one or more WWW-Authenticate headers. If the server challenges with multiple Digest headers, then each one of these headers MUST use a different digest algorithm. The server MUST add these Digest headers to the response in order of preference, starting with the most preferred header, followed by the less preferred headers.

This specification defines the following preference list, starting with the most preferred algorithm:

* SHA2-256 as the default algorithm.
* SHA2-512/256 as a backup algorithm.
* MD5 for backward compatibility.

A future version of this document might add SHA3 [SHA3] as a backup algorithm, once its definition has been finalized and published.

When the client receives the response it SHOULD use the topmost header that it supports, unless a local policy dictates otherwise. The client should ignore any challenge it does not understand.

3.8 Proxy-Authentication and Proxy-Authorization

The digest authentication scheme may also be used for authenticating users to proxies, proxies to proxies, or proxies to origin servers by use of the Proxy-Authenticate and Proxy-Authorization headers. These headers are instances of the Proxy-Authenticate and Proxy-Authorization headers specified in sections 10.33 and 10.34 of the HTTP/1.1 specification [RFC2616] and their behavior is subject to restrictions described there. The transactions for proxy authentication are very similar to those already described. Upon receiving a request which requires authentication, the proxy/server must issue the "407 Proxy Authentication Required" response with a "Proxy-Authenticate" header. The digest-challenge used in the Proxy-Authenticate header is the same as that for the WWW- Authenticate

header as defined above in section 3.2.1.

The client/proxy must then re-issue the request with a Proxy-Authorization header, with directives as specified for the Authorization header in section 3.4 above.

On subsequent responses, the server sends Proxy-Authentication-Info with directives the same as those for the Authentication-Info header field.

Note that in principle a client could be asked to authenticate itself to both a proxy and an end-server, but never in the same response.

3.9 Example

The following example assumes that an access protected document is being requested from the server via a GET request. The URI of the document is http://www.nowhere.org/dir/index.html". Both client and server know that the username for this document is "Mufasa" and the password is "Circle of Life" (with one space between each of the three words).

The first time the client requests the document, no Authorization header is sent, so the server responds with:

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest
        realm = "testrealm@host.com",
        qop="auth, auth-int",
        algorithm="SHA2-256",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        opaque="5ccc069c403ebaf9f0171e9517f40e41"
WWW-Authenticate: Digest
        realm="testrealm@host.com",
        qop="auth, auth-int",
        algorithm="MD5",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        opaque="5ccc069c403ebaf9f0171e9517f40ef41"
```

The client may prompt the user for their username and password, after which it will respond with a new request, including the following Authorization header if the client chooses MD5 digest:

```
Authorization:Digest username="Mufasa",
        realm="testrealm@host.com",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        uri="/dir/index.html",
        qop="auth",
        algorithm="MD5",
        nc=00000001,
        cnonce="0a4f113b",
        response="6629fae49393a05397450978507c4ef1",
        opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

If the client chooses to use the SHA2-256 algorithm for calculating the response, the client responds with a new request including the following Authorization header:

```
Authorization:Digest username="Mufasa",
        realm="testrealm@host.com",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        uri="/dir/index.html",
        qop="auth",
        algorithm="SHA2-256",
        nc=00000001,
        cnonce="0a4f113b",
        response="5abdd07184ba512a22c53f41470e5eea7dcaa3a93
                        a59b630c13dfe0a5dc6e38b",
        opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

4 Internationalization

In challenges, servers SHOULD use the "charset" authentication parameter (case-insensitive) to express the character encoding they expect the user agent to use.

The only allowed value is "UTF-8", to be matched case-insensitively, indicating that the server expects the UTF-8 character encoding to be used ([RFC3629]).

If the user agent supports the encoding indicated by the server, it MAY add the "charset" parameter, with the value it received from the server, to the Proxy-Authenticate or WWW-Authenticate header fields it sends back to the server.

If the user agent does not support the encoding indicated by the server, it MAY add the "charset" parameter to the Proxy-Authenticate or WWW-Authenticate header fields it sends back to the server, but the value in the parameter should be preceded by an exclamation point (!).

5 Security Considerations

5.1 Limitations

HTTP Digest authentication, when used with human-memorable passwords, is vulnerable to dictionary attacks. Such attacks are much easier than cryptographic attacks on any widely used algorithm, including those that are no longer considered secure. In other words, algorithm agility does not make this usage any more secure.

As a result, Digest authentication SHOULD be used only with passwords that have a reasonable amount of entropy, e.g. 128-bit or more. Such passwords typically cannot be memorized by humans but can be used for automated web services.

It is recommended that Digest authentication be used over a secure channel like HTTPS.

5.2 Authentication of Clients using Digest Authentication

Digest Authentication does not provide a strong authentication mechanism, when compared to public key based mechanisms, for example.

However, it is significantly stronger than (e.g.) CRAM-MD5, which has been proposed for use with LDAP [10], POP and IMAP (see RFC 2195

[9]). It is intended to replace the much weaker and even more dangerous Basic mechanism.

Digest Authentication offers no confidentiality protection beyond protecting the actual password. All of the rest of the request and response are available to an eavesdropper.

Digest Authentication offers only limited integrity protection for the messages in either direction. If qop=auth-int mechanism is used, those parts of the message used in the calculation of the WWW-Authenticate and Authorization header field response directive values (see section 3.2 above) are protected. Most header fields and their values could be modified as a part of a man-in-the-middle attack.

Many needs for secure HTTP transactions cannot be met by Digest Authentication. For those needs TLS or SHTTP are more appropriate protocols. In particular Digest authentication cannot be used for any transaction requiring confidentiality protection. Nevertheless many functions remain for which Digest authentication is both useful and appropriate. Any service in present use that uses Basic should be switched to Digest as soon as practical.

5.3 Limited Use Nonce Values

The Digest scheme uses a server-specified nonce to seed the generation of the request-digest value (as specified in section 3.2.2.1 above). As shown in the example nonce in section 3.2.1, the server is free to construct the nonce such that it may only be used from a particular client, for a particular resource, for a limited period of time or number of uses, or any other restrictions. Doing so strengthens the protection provided against, for example, replay attacks (see 4.5). However, it should be noted that the method chosen for generating and checking the nonce also has performance and resource implications. For example, a server may choose to allow each nonce value to be used only once by maintaining a record of whether or not each recently issued nonce has been returned and sending a next-nonce directive in the Authentication-Info header field of every response. This protects against even an immediate replay attack, but has a high cost checking nonce values, and perhaps more important will cause authentication failures for any pipelined requests (presumably returning a stale nonce indication). Similarly, incorporating a request-specific element such as the Etag value for a resource limits the use of the nonce to that version of the resource and also defeats pipelining. Thus it may be useful to do so for methods with side effects but have unacceptable performance for those that do not.

5.4 Replay Attacks

A replay attack against Digest authentication would usually be pointless for a simple GET request since an eavesdropper would already have seen the only document he could obtain with a replay. This is because the URI of the requested document is digested in the client request and the server will only deliver that document. By contrast under Basic Authentication once the eavesdropper has the user's password, any document protected by that password is open to him.

Thus, for some purposes, it is necessary to protect against replay attacks. A good Digest implementation can do this in various ways. The server created "nonce" value is implementation dependent, but if it contains a digest of the client IP, a time-stamp, the resource ETag, and a private server key (as recommended above) then a replay attack is not simple. An attacker must convince the server that the request is coming from a false IP address and must cause the server to deliver the document to an IP address different from the address to which it believes it is sending the document. An attack can only succeed in the period before the time-stamp expires. Digesting the client IP and time-stamp in the nonce permits an implementation which does not maintain state between transactions.

For applications where no possibility of replay attack can be tolerated the server can use one-time nonce values which will not be honored for a second use. This requires the overhead of the server

remembering which nonce values have been used until the nonce time-stamp (and hence the digest built with it) has expired, but it effectively protects against replay attacks.

An implementation must give special attention to the possibility of replay attacks with POST and PUT requests. Unless the server employs one-time or otherwise limited-use nonces and/or insists on the use of the integrity protection of qop=auth-int, an attacker could replay valid credentials from a successful request with counterfeit form data or other message body. Even with the use of integrity protection most metadata in header fields is not protected. Proper nonce generation and checking provides some protection against replay of previously used valid credentials, but see 4.8.

5.5 Weakness Created by Multiple Authentication Schemes

An HTTP/1.1 server may return multiple challenges with a 401 (Authenticate) response, and each challenge may use a different auth-scheme. A user agent MUST choose to use the strongest auth- scheme it

understands and request credentials from the user based upon that challenge.

> Note that many browsers will only recognize Basic and will require that it be the first auth-scheme presented. Servers should only include Basic if it is minimally acceptable.

When the server offers choices of authentication schemes using the WWW-Authenticate header, the strength of the resulting authentication is only as good as that of the of the weakest of the authentication schemes. See section 5.7 below for discussion of particular attack scenarios that exploit multiple authentication schemes.

5.6 Online dictionary attacks

If the attacker can eavesdrop, then it can test any overheard nonce/response pairs against a list of common words. Such a list is usually much smaller than the total number of possible passwords. The cost of computing the response for each password on the list is paid once for each challenge.

The server can mitigate this attack by not allowing users to select passwords that are in a dictionary.

5.7 Man in the Middle

Both Basic and Digest authentication are vulnerable to "man in the middle" (MITM) attacks, for example, from a hostile or compromised proxy. Clearly, this would present all the problems of eavesdropping. But it also offers some additional opportunities to the attacker.

A possible man-in-the-middle attack would be to add a weak authentication scheme to the set of choices, hoping that the client will use one that exposes the user's credentials (e.g. password). For this reason, the client should always use the strongest scheme that it understands from the choices offered.

An even better MITM attack would be to remove all offered choices, replacing them with a challenge that requests only Basic authentication, then uses the cleartext credentials from the Basic authentication to authenticate to the origin server using the stronger scheme it requested. A particularly insidious way to mount such a MITM attack would be to offer a "free" proxy caching service to gullible users.

User agents should consider measures such as presenting a visual

indication at the time of the credentials request of what authentication scheme is to be used, or remembering the strongest authentication scheme ever requested by a server and produce a warning message before using a weaker one. It might also be a good idea for the user agent to be configured to demand Digest authentication in general, or from specific sites.

Or, a hostile proxy might spoof the client into making a request the attacker wanted rather than one the client wanted. Of course, this is still much harder than a comparable attack against Basic Authentication.

5.8 Chosen plaintext attacks

With Digest authentication, a MITM or a malicious server can arbitrarily choose the nonce that the client will use to compute the response. This is called a "chosen plaintext" attack. The ability to choose the nonce is known to make cryptanalysis much easier [8].

However, no way to analyze the MD5 one-way function used by Digest using chosen plaintext is currently known.

The countermeasure against this attack is for clients to be configured to require the use of the optional "cnonce" directive; this allows the client to vary the input to the hash in a way not chosen by the attacker.

5.9 Precomputed dictionary attacks

With Digest authentication, if the attacker can execute a chosen plaintext attack, the attacker can precompute the response for many common words to a nonce of its choice, and store a dictionary of (response, password) pairs. Such precomputation can often be done in parallel on many machines. It can then use the chosen plaintext attack to acquire a response corresponding to that challenge, and just look up the password in the dictionary. Even if most passwords are not in the dictionary, some might be. Since the attacker gets to pick the challenge, the cost of computing the response for each password on the list can be amortized over finding many passwords. A dictionary with 100 million password/response pairs would take about 3.2 gigabytes of disk storage.

The countermeasure against this attack is to for clients to be configured to require the use of the optional "cnonce" directive.

5.10 Batch brute force attacks

With Digest authentication, a MITM can execute a chosen plaintext attack, and can gather responses from many users to the same nonce. It can then find all the passwords within any subset of password space that would generate one of the nonce/response pairs in a single pass over that space. It also reduces the time to find the first password by a factor equal to the number of nonce/response pairs gathered. This search of the password space can often be done in parallel on many machines, and even a single machine can search large subsets of the password space very quickly -- reports exist of searching all passwords with six or fewer letters in a few hours.

The countermeasure against this attack is to for clients to be configured to require the use of the optional "cnonce" directive.

5.11 Spoofing by Counterfeit Servers

Basic Authentication is vulnerable to spoofing by counterfeit servers. If a user can be led to believe that she is connecting to a host containing information protected by a password she knows, when in fact she is connecting to a hostile server, then the hostile server can request a password, store it away for later use, and feign an error. This type of attack is more difficult with Digest Authentication -- but the client must know to demand that Digest authentication be used, perhaps using some of the techniques described above to counter "man-in-the-middle" attacks. Again, the user can be helped in detecting this attack by a visual indication of the authentication mechanism in use with appropriate guidance in interpreting the implications of each scheme.

5.12 Storing passwords

Digest authentication requires that the authenticating agent (usually the server) store some data derived from the user's name and password in a "password file" associated with a given realm. Normally this might contain pairs consisting of username and H(A1), where H(A1) is the digested value of the username, realm, and password as described above.

The security implications of this are that if this password file is compromised, then an attacker gains immediate access to documents on the server using this realm. Unlike, say a standard UNIX password file, this information need not be decrypted in order to access documents in the server realm associated with this file. On the other hand, decryption, or more likely a brute force attack, would be

necessary to obtain the user's password. This is the reason that the realm is part of the digested data stored in the password file. It means that if one Digest authentication password file is compromised, it does not automatically compromise others with the same username and password (though it does expose them to brute force attack).

There are two important security consequences of this. First the password file must be protected as if it contained unencrypted passwords, because for the purpose of accessing documents in its realm, it effectively does.

A second consequence of this is that the realm string should be unique among all realms which any single user is likely to use. In particular a realm string should include the name of the host doing the authentication. The inability of the client to authenticate the server is a weakness of Digest Authentication.

5.13 Summary

By modern cryptographic standards Digest Authentication is weak. But for a large range of purposes it is valuable as a replacement for Basic Authentication. It remedies some, but not all, weaknesses of Basic Authentication. Its strength may vary depending on the implementation. In particular the structure of the nonce (which is dependent on the server implementation) may affect the ease of mounting a replay attack. A range of server options is appropriate since, for example, some implementations may be willing to accept the server overhead of one-time nonces or digests to eliminate the possibility of replay. Others may satisfied with a nonce like the one recommended above restricted to a single IP address and a single ETag or with a limited lifetime.

The bottom line is that *any* compliant implementation will be relatively weak by cryptographic standards, but *any* compliant implementation will be far superior to Basic Authentication.

6 IANA Considerations

This specification creates a new IANA registry named "HTTP Digest Hash Algorithms". When registering a new hash algorithm, the following information MUST be provided:

- The textual name of the hash algorithm.
- A reference to the specification that describes the new algorithm.

The update policy for this registry shall be Specification Required.

The initial registry will contain the following entries:

Hash Algorithm	Reference
"MD5"	RFC XXXX
"MD5-sess"	RFC XXXX
"SHA2-256"	RFC XXXX
"SHA2-256-sess"	RFC XXXX
"SHA2-512-256"	RFC XXXX
"SHA2-512-256-sess"	RFC XXXX

7 Acknowledgments

TODO

8 References

8.1 Normative References

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

[RFC1776] Crocker, S., "The Address is the Message", RFC 1776, April 1 1995.

[TRUTHS] Callon, R., "The Twelve Networking Truths", RFC 1925, April 1 1996.

8.2 Informative References

[EVILBIT] Bellovin, S., "The Security Flag in the IPv4 Header", RFC 3514, April 1 2003.

[RFC5513] Farrel, A., "IANA Considerations for Three Letter Acronyms", RFC 5513, April 1 2009.

[RFC5514] Vyncke, E., "IPv6 over Social Networks", RFC 5514, April 1 2009.

Authors' Addresses

Rifaat Shekh-Yusef (Editor)
Avaya
250 Sydney Street
Belleville, Ontario
Canada

Phone: +1-613-967-5267
Email: rifaat.ietf@gmail.com

David Ahrens
Avaya
California
USA

EMail: ahrensdc@gmail.com

Sophie Bremer
Netzkonform
Germany

Email: sophie.bremer@netzkonform.de