Table of Contents

原文链接：https://tools.ietf.org/rfc/rfc2617.txt 翻译：qunfanyi.com

1 Access Authentication

1.1 Reliance on the HTTP/1.1 Specification

~~[en]This specification is a companion to the HTTP/1.1 specification [2].~~
本规范是HTTP／1.1规范（2）的伙伴。

~~[en]It uses the augmented BNF section 2.1 of that document, and relies on both the non-terminals defined in that document and other aspects of the HTTP/1.1 specification.~~
它使用该文档的扩展BNF部分2.1，并且依赖于该文档中定义的非终端以及HTTP/1.1规范的其他方面。

1.2 Access Authentication Framework

[en]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.
HTTP提供了一种简单的质询-响应身份验证机制，服务器可以使用该机制来质询客户机请求，客户机可以使用该机制来提供身份验证信息。

[en]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.
它使用一个可扩展的、不区分大小写的令牌来标识身份验证方案，然后是属性值对的逗号分隔列表，该列表携带通过该方案实现身份验证所需的参数。

[en]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.
auth-.=token auth-param=token"="(token|quoted-string)401(Unauthor.)响应消息被源服务器用来挑战用户代理的授权。

[en]This response MUST include a WWW-Authenticate header field containing at least one challenge applicable to the requested resource.
该响应必须包括WWW认证标头字段，该字段包含至少一个适用于所请求资源的挑战。

[en]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.
代理使用407(代理身份验证要求)响应消息来挑战客户端的授权，并且必须包括代理身份验证报头字段，该报头字段包含至少一个适用于请求资源的代理的挑战。

[en]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.
.=auth-scheme 1*SP 1#auth-param注意：如果WWW-Authenticate或Proxy-Authenticate报头字段包含不止一个查询，或者如果提供了不止一个WWW-Authenticate报头字段，则用户代理将需要在解析WWW-Authenticate或Proxy-Authenticate报头字段值时特别小心，因为查询的内容是GE本身可能包含一个逗号分隔的认证参数列表。

[en]The authentication parameter realm is defined for all authentication schemes: realm = "realm" "=" realm-value realm-value = quoted-string Franks, et al.
身份验证参数realm是为所有身份验证方案定义的：realm="realm"="realm-value realm-value=quoted-string Franks，等等。

[en]Standards Track [Page 3] RFC 2617 HTTP Authentication June 1999 The realm directive (case-insensitive) is required for all authentication schemes that issue a challenge.
标准跟踪[第3页]RFC 2617 HTTP认证1999年6月域指令（不区分大小写）对于发出挑战的所有认证方案是必需的。

[en]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 [2]) of the server being accessed, defines the protection space.
领域值（区分大小写）与被访问的服务器的标准根URL（abs_path为空的服务器的绝对URI；参见[2]的第5.1.2节）组合定义了保护空间。

[en]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.
这些域允许将服务器上的受保护资源划分为一组保护空间，每个保护空间具有自己的身份验证方案和/或授权数据库。

[en]The realm value is a string, generally assigned by the origin server, which may have additional semantics specific to the authentication scheme.
领域值是一个字符串，通常由源服务器分配，该字符串可能具有特定于身份验证方案的附加语义。

[en]Note that there may be multiple challenges with the same auth-scheme but different realms.
注意，相同的AUTH方案可能有多个挑战，但是不同的领域。

[en]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.
希望通过原始服务器进行自身身份验证的用户代理——通常在接收到401（未授权）之后，但不是必须——可以通过在请求中包括授权头部字段来进行身份验证。

[en]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.
希望通过代理进行自身身份验证的客户机——通常在接收到407（需要代理身份验证）之后但不一定——可以通过在请求中包含代理授权头部字段来进行身份验证。

[en]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.
Authorization字段值和Proxy-Authorization字段值都由包含请求的资源领域的客户端身份验证信息的凭证组成。

[en]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.
用户代理必须选择使用它所理解的最强认证方案的挑战之一，并基于该挑战向用户请求凭证。

[en]credentials = auth-scheme #auth-param Note that many browsers will only recognize Basic and will require that it be the first auth-scheme presented.
凭据＝AuthPosivayAuthPARAM注意到，许多浏览器只会识别BASIC，并要求它是第一个AUTH方案。

[en]Servers should only include Basic if it is minimally acceptable.
如果最低限度的接受，服务器应该只包括BASIC。

[en]The protection space determines the domain over which credentials can be automatically applied.
保护空间决定可以自动应用凭据的域。

[en]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.
如果先前的请求已经被授权，则相同的凭证可以在由认证方案、参数和/或用户偏好确定的时间段内对该保护空间内的所有其他请求重用。

[en]Unless otherwise defined by the authentication scheme, a single protection space cannot extend outside the scope of its server.
除非认证方案另有定义，否则单个保护空间不能扩展到其服务器的范围之外。

[en]If the origin server does not wish to accept the credentials sent with a request, it SHOULD return a 401 (Unauthorized) response.
如果源服务器不希望接受请求发送的凭据，则应该返回401（未授权）响应。

[en]The response MUST include a WWW-Authenticate header field containing at least one (possibly new) challenge applicable to the requested resource.
响应必须包括WWW-Authenticate报头字段，其中包含至少一个（可能是新的）适用于所请求资源的挑战。

[en]If a proxy does not accept the credentials sent with a request, it SHOULD return a 407 (Proxy Authentication Required).
如果代理不接受请求发送的凭据，则应该返回407（需要代理身份验证）。

[en]The response MUST include a Proxy-Authenticate header field containing a Franks, et al.
响应必须包括包含弗兰克斯等的代理认证头字段。

[en]Standards Track [Page 4] RFC 2617 HTTP Authentication June 1999 (possibly new) challenge applicable to the proxy for the requested resource.
标准跟踪[第4页]RFC 2617 HTTP身份验证1999年6月（可能是新的）挑战，适用于请求资源的代理。

[en]The HTTP protocol does not restrict applications to this simple challenge-response mechanism for access authentication.
HTTP协议不将应用程序限制为用于访问认证的这种简单的挑战响应机制。

[en]Additional mechanisms MAY be used, such as encryption at the transport level or via message encapsulation, and with additional header fields specifying authentication information.
可以使用其他机制，例如在传输级别或通过消息封装进行加密，以及使用指定身份验证信息的附加头部字段。

[en]However, these additional mechanisms are not defined by this specification.
然而，这些额外的机制不是由本规范定义的。

[en]Proxies MUST be completely transparent regarding user agent authentication by origin servers.
代理必须完全透明关于源代理的用户代理身份验证。

[en]That is, they must forward the WWW-Authenticate and Authorization headers untouched, and follow the rules found in section 14.8 of [2].
也就是说，它们必须不加修改地转发WWW-Authenticate和Authorization报头，并遵循[2]第14.8节中的规则。

[en]Both the Proxy-Authenticate and the Proxy-Authorization header fields are hop-by-hop headers (see section 13.5.1 of [2]).
代理认证和代理授权标头字段都是逐跳标头（参见[135.1的[2）]。

2 Basic Authentication Scheme

~~[en]The "basic" authentication scheme is based on the model that the client must authenticate itself with a user-ID and a password for each realm.~~
“基本”身份验证方案基于这样的模型，即客户端必须使用每个域的用户ID和密码进行身份验证。

~~[en]The realm value should be considered an opaque string which can only be compared for equality with other realms on that server.~~
域值应该被认为是一个不透明的字符串，只能与该服务器上的其他领域进行比较。

~~[en]The server will service the request only if it can validate the user-ID and password for the protection space of the Request-URI.~~
只有当服务器能够验证请求URI的保护空间的用户ID和密码时，服务器才会服务该请求。

~~[en]There are no optional authentication parameters.~~
没有可选的身份验证参数。

~~[en]For Basic, the framework above is utilized as follows: challenge = "Basic" realm credentials = "Basic" basic-credentials Upon receipt of an unauthorized request for a URI within the protection space, the origin server MAY respond with a challenge like the following: WWW-Authenticate: Basic realm="WallyWorld" where "WallyWorld" is the string assigned by the server to identify the protection space of the Request-URI.~~
对于Basic，上面的框架被利用如下：.="Basic"领域凭证="Basic"基本凭证。当接收到对保护空间内的URI的未经授权的请求时，原始服务器可能以如下挑战来响应：WWW-Authenticate：Basic领域="W“WalyWord”所在的“WalyWord”是由服务器分配的字符串，用于标识请求URI的保护空间。

~~[en]A proxy may respond with the same challenge using the Proxy-Authenticate header field.~~
代理可以使用代理认证头字段响应相同的挑战。

~~[en]To receive authorization, the client sends the userid and password, separated by a single colon (":") character, within a base64 [7] encoded string in the credentials.~~
为了接收授权，客户端在凭据中的base64[7]编码字符串内发送用户标识和密码，用户标识和密码由单个冒号(":")字符分隔。

~~[en]basic-credentials = base64-user-pass base64-user-pass = <base64 [4] encoding of user-pass, Franks, et al.~~
基本凭据＝Base64用户通过Base64用户PASS＝BASE64（4）用户通过的编码，弗兰克斯等人。

~~[en]Standards Track [Page 5] RFC 2617 HTTP Authentication June 1999 except not limited to 76 char/line> user-pass = userid ":" password userid = *password* = TEXT Userids might be case sensitive.~~
标准跟踪[第5页]RFC 2617 HTTP身份验证1999年6月，除了不限于76个字符/行>user-pass=userid":"password userid=<_ *class="calibre13">password*=TEXT Userids可能是区分大小写的。

~~[en]If the user agent wishes to send the userid "Aladdin" and password "open sesame", it would use the following header field: Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ== A client SHOULD assume that all paths at or deeper than the depth of the last symbolic element in the path field of the Request-URI also are within the protection space specified by the Basic realm value of the current challenge.~~
如果用户代理希望发送用户标识“Aladdin”和密码“opense.”，它将使用以下标题字段：Authorization：BasicQWxhZGRpjpjpvcGVlHNlc2FtZQ==客户端应该假设所有路径位于请求的路径字段中的最后一个符号元素的深度或更深T-URI也在由当前挑战的基本域值指定的保护空间内。

~~[en]A client MAY preemptively send the corresponding Authorization header with requests for resources in that space without receipt of another challenge from the server.~~
客户机可以抢先发送相应的授权报头，其中包含对该空间中的资源的请求，而无需接收来自服务器的另一个挑战。

[en]Similarly, when a client sends a request to a proxy, it may reuse a userid and password in the Proxy-Authorization header field without receiving another challenge from the proxy server.
类似地，当客户机向代理发送请求时，它可以在代理授权头部字段中重用用户标识和密码，而不会从代理服务器接收另一个挑战。

[en]See section 4 for security considerations associated with Basic authentication.
有关与基本身份验证相关的安全考虑，请参见第4节。

3 Digest Access Authentication Scheme

3.1 Introduction

3.1.1 Purpose

~~[en]The protocol referred to as "HTTP/1.0" includes the specification for a Basic Access Authentication scheme[1].~~
称为“HTTP／1”的协议包括基本接入认证方案的规范[1]。

~~[en]That scheme is not considered to be a secure method of user authentication, as the user name and password are passed over the network in an unencrypted form.~~
由于用户名和密码以未加密的形式在网络上传递，因此该方案不被认为是用户身份验证的安全方法。

~~[en]This section provides the specification for a scheme that does not send the password in cleartext, referred to as "Digest Access Authentication".~~
本节提供了不在CytTress中发送密码的方案的规范，称为“摘要访问认证”。

~~[en]The Digest Access Authentication scheme is not intended to be a complete answer to the need for security in the World Wide Web.~~
摘要访问认证方案不打算是万维网安全需求的完全答案。

~~[en]This scheme provides no encryption of message content.~~
该方案不提供消息内容的加密。

~~[en]The intent is simply to create an access authentication method that avoids the most serious flaws of Basic authentication.~~
目的是创建一个访问认证方法，避免了基本认证的最严重缺陷。

3.1.2 Overall Operation

~~[en]Like Basic Access Authentication, the Digest scheme is based on a simple challenge-response paradigm.~~
与基本的访问认证一样，摘要方案基于简单的挑战-响应范例。

~~[en]The Digest scheme challenges using a nonce value.~~
摘要方案使用NOCE值进行挑战。

~~[en]A valid response contains a checksum (by Franks, et al.~~
一个有效的响应包含校验和（由弗兰克斯等人）。

~~[en]Standards Track [Page 6] RFC 2617 HTTP Authentication June 1999 default, the MD5 checksum) of the username, the password, the given nonce value, the HTTP method, and the requested URI.~~
标准跟踪[第6页]RFC 2617 HTTP身份验证，1999年6月默认，MD5校验和）的用户名、密码、给定的临时值、HTTP方法和请求的URI。

~~[en]In this way, the password is never sent in the clear.~~
这样，密码就不会在清除中发送。

~~[en]Just as with the Basic scheme, the username and password must be prearranged in some fashion not addressed by this document.~~
正如基本方案一样，用户名和密码必须以某种方式预先安排，而不是本文档所处理的。

3.1.3 Representation of digest values

~~[en]An optional header allows the server to specify the algorithm used to create the checksum or digest.~~
可选的头允许服务器指定用于创建校验和或摘要的算法。

~~[en]By default the MD5 algorithm is used and that is the only algorithm described in this document.~~
默认情况下，使用MD5算法，这是本文档中描述的唯一算法。

~~[en]For the purposes of this document, an MD5 digest of 128 bits is represented as 32 ASCII printable characters.~~
为了本文档的目的，128位的MD5摘要被表示为32个ASCII可打印字符。

~~[en]The bits in the 128 bit digest are converted from most significant to least significant bit, four bits at a time to their ASCII presentation as follows.~~
128位摘要中的位从最高有效位转换为最低有效位，每次4位转换为它们的ASCII表示如下。

~~[en]Each four bits is represented by its familiar hexadecimal notation from the characters 0123456789abcdef.~~
每个四位用其熟悉的十六进制表示法从字符012345 67 89ABCDEF表示。

~~[en]That is, binary 0000 gets represented by the character '0', 0001, by '1', and so on up to the representation of 1111 as 'f'.~~
也就是说，二进制0000由字符“0”、“0001”、“1”等表示，直到1111表示为“f”。

3.1.4 Limitations

~~[en]The Digest authentication scheme described in this document suffers from many known limitations.~~
本文档中描述的摘要认证方案遭受许多已知的限制。

~~[en]It is intended as a replacement for Basic authentication and nothing more.~~
它的目的是作为基本身份验证的替代品。

~~[en]It is a password-based system and (on the server side) suffers from all the same problems of any password system.~~
它是一个基于密码的系统，并且（在服务器端）遭受任何密码系统的所有相同的问题。

~~[en]In particular, no provision is made in this protocol for the initial secure arrangement between user and server to establish the user's password.~~
特别地，本协议中没有规定在用户和服务器之间建立用户密码的初始安全安排。

~~[en]Users and implementors should be aware that this protocol is not as secure as Kerberos, and not as secure as any client-side private-key scheme.~~
用户和实现者应该知道，这个协议不像Kerberos那么安全，也不像任何客户端私钥方案那么安全。

~~[en]Nevertheless it is better than nothing, better than what is commonly used with telnet and ftp, and better than Basic authentication.~~
尽管如此，它总比什么都不做好，比telnet和ftp通常使用的要好，也比基本身份验证要好。

3.2 Specification of Digest Headers

~~[en]The Digest Access Authentication scheme is conceptually similar to the Basic scheme.~~
摘要访问认证方案在概念上类似于基本方案。

~~[en]The formats of the modified WWW-Authenticate header line and the Authorization header line are specified below.~~
修改WWW认证标题行和授权标题行的格式如下所示。

~~[en]In addition, a new header, Authentication-Info, is specified.~~
另外，指定了一个新的报头，即身份验证信息。

~~[en]Franks, et al.~~
弗兰克斯等。

3.2.1 The WWW-Authenticate Response Header

~~[en]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] | [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" | token) qop-options = "qop" "=" <"> 1#qop-value <"> qop-value = "auth" | "auth-int" | token 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.~~
如果服务器接收到对受访问保护对象的请求，并且不发送可接受的授权标头，则服务器以“401未授权”状态代码响应，并且根据上述定义的WWW认证报头，对于摘要方案，使用如下：ge ge= "Digest"摘要-挑战摘要-挑战摘要-摘要-挑战-摘要-摘要-挑战-摘要=1#(realm.....[[..[[[.摘要.摘要.摘要.摘要.摘要.摘要.摘要.摘要挑战摘要摘要摘要摘要摘要摘要摘要摘要摘要挑战摘要摘要摘要摘要摘要摘要挑战摘要摘要挑战摘要摘要摘要摘要挑战摘要摘要摘要摘要摘要摘要摘要摘要摘要挑战摘要摘要摘要摘要摘要摘要摘要挑战挑战挑战摘要摘要摘要摘要挑战摘要摘要摘要摘要摘要摘要摘要摘要摘要摘要挑战挑战挑战摘要摘要摘要摘要摘要摘要摘要摘要摘要摘要摘要摘要摘要摘要挑战挑战挑战que的=“不透明”=“引用字符串过时”=“陈旧”“=”（“真”“假”）算法=“算法”“=”（“MD5”“MD5 SESS”“令牌”）QOP选项＝“QOP”=“<”＞1“QOP值< AQTH值”“AUTH INTING”令牌上述指令值的含义如下：要显示给用户，以便他们知道要使用的用户名和密码。

~~[en]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.~~
该字符串应该至少包含执行身份验证的主机的名称，并且可能另外指示可能具有访问权限的用户的集合。

~~[en]An example might be "registered_users@gotham.news.com".~~
一个例子可能是“RealStEdSuffer-@ GothAM.News .com”。

~~[en]domain A quoted, space-separated list of URIs, as specified in RFC XURI [7], that define the protection space.~~
域中引用的一个空间分隔的URI列表，如RFC XURI（7）中规定的，定义了保护空间。

~~[en]If a URI is an abs_path, it is relative to the canonical root URL (see section 1.2 above) of the server being accessed.~~
如果URI是AbsPyPATH，则与正在访问的服务器的规范根URL（参见上面的第1.2节）有关。

~~[en]An absoluteURI in this list may refer to a different server than the one being accessed.~~
此列表中的Abjuturi可能指的是与正在访问的服务器不同的服务器。

~~[en]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.~~
客户端可以使用该列表来确定可以发送相同身份验证信息的URI集合：可以将此列表中具有URI作为前缀的任何URI（在这两个URI都成为绝对值之后）假定在相同的保护空间中。

~~[en]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.~~
如果该指令被省略或者它的值是空的，客户端应该假定保护空间由响应服务器上的所有URI组成。

~~[en]Franks, et al.~~
弗兰克斯等。

~~[en]Standards Track [Page 8] RFC 2617 HTTP Authentication June 1999 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.~~
标准跟踪[第8页]RFC 2617HTTP认证1999年6月本指令在代理-认证报头中没有意义，对于代理-认证报头，保护空间总是整个代理；如果存在，则应该忽略它。

~~[en]nonce A server-specified data string which should be uniquely generated each time a 401 response is made.~~
NoCE一个服务器指定的数据字符串，在每次做出401响应时，它应该是唯一生成的。

~~[en]It is recommended that this string be base64 or hexadecimal data.~~
建议此字符串为Base64或十六进制数据。

~~[en]Specifically, since the string is passed in the header lines as a quoted string, the double-quote character is not allowed.~~
具体来说，由于字符串在标题行中作为引用字符串传递，因此不允许双引号字符。

~~[en]The contents of the nonce are implementation dependent.~~
NANCE的内容是依赖于实现的。

~~[en]The quality of the implementation depends on a good choice.~~
实施的质量取决于一个好的选择。

~~[en]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.~~
例如，一个nonce可以被构造为时间戳H（时间戳“:”ETag“:”私钥）的基础64编码，其中时间戳是服务器生成的时间或其他非重复值，ETag是与请求实体相关联的HTTP ETag报头的值，私钥是数据k仅限于服务器。

~~[en]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.~~
对于这种形式的nonce，服务器在接收到客户端身份验证头部之后将重新计算哈希部分，如果该请求与来自该头部的nonce不匹配，或者如果时间戳值不够新，则拒绝该请求。

~~[en]In this way the server can limit the time of the nonce's validity.~~
这样，服务器可以限制NoCE有效性的时间。

~~[en]The inclusion of the ETag prevents a replay request for an updated version of the resource.~~
包含ETAG防止对资源的更新版本的重放请求。

~~[en](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.~~
（注意：在nonce中包括客户端的IP地址似乎可以提供服务器将nonce的重用限制到最初得到它的同一客户端的能力）。

~~[en]However, that would break proxy farms, where requests from a single user often go through different proxies in the farm.~~
然而，这将破坏代理农场，其中来自单个用户的请求经常在农场中通过不同代理。

~~[en]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.~~
同样，IP地址欺骗也不是那么难。）实现可能选择不接受先前使用的nonce或先前使用的摘要，以便防止重播攻击。

~~[en]Or, an implementation might choose to use one-time nonces or digests for POST or PUT requests and a time-stamp for GET requests.~~
或者，一个实现可能会选择使用一次性或抽象的POST或PUT请求和GET请求的时间戳。

~~[en]For more details on the issues involved see section 4.~~
有关问题的更多细节见第4节。

[en]of this document.
这份文件。

[en]The nonce is opaque to the client.
客户机的不透明是不透明的。

[en]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.
不透明的：由服务器指定的数据字符串，客户端应在具有相同保护空间中的URI的后续请求的授权头中原封不动地返回该字符串。

[en]It is recommended that this string be base64 or hexadecimal data.
建议此字符串为Base64或十六进制数据。

[en]Franks, et al.
弗兰克斯等。

[en]Standards Track [Page 9] RFC 2617 HTTP Authentication June 1999 stale A flag, indicating that the previous request from the client was rejected because the nonce value was stale.
Standards Track[Page 9]RFC 2617 HTTP Authentication 1999年6月过时A标志，指示来自客户端的上一次请求被拒绝，因为nonce值过时。

[en]If stale is TRUE (case-insensitive), the client may wish to simply retry the request with a new encrypted response, without reprompting the user for a new username and password.
如果过期为真（区分大小写），则客户端可能希望仅使用新的加密响应重试请求，而不会为新的用户名和密码重新注册用户。

[en]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).
如果服务器接收到nonce无效但具有该nonce的有效摘要（指示客户端知道正确的用户名/密码）的请求，则服务器应该将stale设置为TRUE。

[en]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.
如果stale是FALSE，或者除了TRUE之外的任何内容，或者没有出现stale指令，则用户名和/或密码无效，并且必须获得新值。

[en]algorithm A string indicating a pair of algorithms used to produce the digest and a checksum.
表示用于生成摘要和校验和的一对算法的字符串。

[en]If this is not present it is assumed to be "MD5".
如果不存在，则假设为“MD5”。

[en]If the algorithm is not understood, the challenge should be ignored (and a different one used, if there is more than one).
如果算法不被理解，则应该忽略该挑战（如果存在不止一个，则使用不同的算法）。

[en]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).
在本文档中，通过将摘要算法应用于具有秘密“.”的数据“data”而获得的字符串将由KD(.，data)表示，并且通过将校验和算法应用于数据“data”而获得的字符串将由H(data)表示。

[en]The notation unq(X) means the value of the quoted-string X without the surrounding quotes.
符号UNQ（x）表示引用的字符串x的值，没有周围的引号。

[en]For the "MD5" and "MD5-sess" algorithms H(data) = MD5(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.
对于“MD5”和“MD5-sess”算法，H(data)=MD5(data)和KD(.，data)=H(concat(.，":，data))，即，摘要是与与数据连接的冒号连接的秘密的MD5。

[en]The "MD5-sess" algorithm is intended to allow efficient 3rd party authentication servers; for the difference in usage, see the description in section 3.2.2.2.
“MD5-sess”算法旨在允许高效的第三方身份验证服务器；有关使用上的差异，请参阅3.2.2.2节中的描述。

[en]qop-options This directive is optional, but is made so only for backward compatibility with RFC 2069 [6]; it SHOULD be used by all implementations compliant with this version of the Digest scheme.
qop-.这个指令是可选的，但是只是为了与RFC 2069[6]向后兼容才这样做的；它应该被符合这个版本的摘要方案的所有实现使用。

[en]If present, it is a quoted string of one or more tokens indicating the "quality of protection" values supported by the server.
如果存在，它是引用一个或多个令牌的字符串，指示服务器支持的“保护质量”值。

[en]The value "auth" indicates authentication; the value "auth-int" indicates authentication with integrity protection; see the Franks, et al.
值“auth”表示身份验证；值“auth-int”表示具有完整性保护的身份验证；参见Franks等。

[en]Standards Track [Page 10] RFC 2617 HTTP Authentication June 1999 descriptions below for calculating the response directive value for the application of this choice.
标准跟踪[第10页]RFC 2617HTTP认证1999年6月，用于计算用于应用该选择的响应指令值的以下描述。

[en]Unrecognized options MUST be ignored.
不可识别的选项必须被忽略。

[en]auth-param This directive allows for future extensions.
AuthPARAM此指令允许将来的扩展。

[en]Any unrecognized directive MUST be ignored.
任何未被识别的指令都必须被忽略。

3.2.2 The Authorization Request Header

[en]The client is expected to retry the request, passing an Authorization header line, which is defined according to the framework above, utilized as follows.
期望客户机重试请求，传递根据上述框架定义的授权标题行，如下所示。

[en]credentials = "Digest" digest-response digest-response = 1#(username | realm | nonce | digest-uri | response | [algorithm] | [cnonce] | [opaque] | [message-qop] | [nonce-count] | [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 = <"> 32LHEX <"> LHEX = "0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" | "8" | "9" | "a" | "b" | "c" | "d" | "e" | "f" The values of the opaque and algorithm fields must be those supplied in the WWW-Authenticate response header for the entity being requested.
凭证="Digest"摘要响应摘要响应=1#(用户名|领域|nonce|digest-uri|响应|[算法]|[cnonce]|[不透明]|[message-qop]|[nonce-count]|[auth-param])用户名="用户名-值用户名-值=引号字符串摘要uri="digest-uri"="digest-uri"="digest-uri-value digest-uri-value=request-uri；如HTTP/1.1消息所指定的，qop="qop"="qop-value cnonce="cnonce"="cnonce-value cnonce-value=nonce-count="nc-value nc-value=8LHEX.="."="request-digest= <">32LHEX<">LHEX="0"|“1”|“2”|“3”|“4”|“6”|“7”|“8”|“9”|“a”|“b”|“c”|“d”|“e”|“f”不透明字段和算法字段的值必须是请求实体的WWW-Authenticate响应头中提供的值。

[en]response A string of 32 hex digits computed as defined below, which proves that the user knows a password username The user's name in the specified realm.
响应32个十六进制数字的字符串，如下面定义的那样计算，这证明用户知道密码用户名。

[en]Franks, et al.
弗兰克斯等。

[en]Standards Track [Page 11] RFC 2617 HTTP Authentication June 1999 digest-uri The URI from Request-URI of the Request-Line; duplicated here because proxies are allowed to change the Request-Line in transit.
标准轨道[页面11] RFC 2617 HTTP认证1999年6月摘要URI URL来自请求线的请求URI；在这里复制，因为代理被允许在传输过程中改变请求线。

[en]qop Indicates what "quality of protection" the client has applied to the message.
QOP指明了客户端应用于消息的“保护质量”。

[en]If present, its value MUST be one of the alternatives the server indicated it supports in the WWW-Authenticate header.
如果存在，它的值必须是服务器在WWW认证头中支持的替代方案之一。

[en]These values affect the computation of the request-digest.
这些值影响请求摘要的计算。

[en]Note that this is a single token, not a quoted list of alternatives as in WWW- Authenticate.
注意，这是一个单一令牌，而不是在WWW认证中引用的备选列表。

[en]This directive is optional in order to preserve backward compatibility with a minimal implementation of RFC 2069 [6], but SHOULD be used if the server indicated that qop is supported by providing a qop directive in the WWW-Authenticate header field.
该指令是可选的，以便保持与RFC 2069[6]的最小实现的向后兼容性，但是如果服务器指示通过在WWW-Authenticate报头字段中提供qop指令来支持qop，则应该使用该指令。

[en]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.
如果发送了qop指令，则必须指定（参见上文），如果服务器在WWW-Authenticate头部字段中没有发送qop指令，则必

须不指定。

[en]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.
cnonce-value是客户机提供的不透明的引用字符串值，客户机和服务器都使用该值来避免所选择的明文攻击、提供相互身份验证以及提供一些消息完整性保护。

[en]See the descriptions below of the calculation of the response- digest and request-digest values.
请参见下面的计算-摘要和请求摘要值的说明。

[en]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.
如果发送了qop指令，则必须指定（参见上文），如果服务器没有在WWW-Authenticate报头字段中发送qop指令，则必须不指定。

[en]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.
nc值是客户机发送的请求数量（包括当前请求）的十六进制计数，其中包含该请求中的nonce值。

[en]For example, in the first request sent in response to a given nonce value, the client sends "nc=00000001".
例如，在响应给定的随机值发送的第一个请求中，客户端发送“NC＝0000000 1”。

[en]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.
这个指令的目的是允许服务器通过维护其自己的计数副本来检测请求重放——如果相同的nc值被看到两次，那么该请求就是重放。

[en]See the description below of the construction of the request-digest value.
请参见下面的请求摘要值的构造说明。

[en]auth-param This directive allows for future extensions.
AuthPARAM此指令允许将来的扩展。

[en]Any unrecognized directive MUST be ignored.
任何未被识别的指令都必须被忽略。

[en]If a directive or its value is improper, or required directives are missing, the proper response is 400 Bad Request.
如果指令或其值不正确，或缺少指令，则正确的响应是400坏请求。

[en]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.
如果请求摘要无效，则应记录登录失败，因为来自单个客户端的重复登录失败可能指示攻击者试图猜测密码。

[en]Franks, et al.
弗兰克斯等。

[en]Standards Track [Page 12] RFC 2617 HTTP Authentication June 1999 The definition of request-digest above indicates the encoding for its value.
标准跟踪[第12页]RFC 2617 HTTP认证1999年6月以上请求摘要的定义表明其值的编码。

[en]The following definitions show how the value is computed.
下面的定义显示了如何计算值。

3.2.2.1 Request-Digest

~~[en]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.~~
如果“qop”值是“auth”或“auth-int”：request-digest=<"><___nc-value_____unq_cnonce-value_____unq_qop-value_____h_a2___ class="calibre13">“qop”指令不存在(此构造用于与RFC 2069兼容)：request-digest=<"> < >参见A1和A2的定义。

3.2.2.2 A1

[en]If the "algorithm" directive's value is "MD5" or is unspecified, 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", then A1 is calculated only once - on the first request by the client following receipt of a WWW-Authenticate challenge from the server.
如果“.”指令的值是“MD5”或未指定，那么A1是：A1=unq（用户名-值）:“unq（领域值）”:“passwd，其中passwd=<用户密码>。从服务器接收WWW认证的挑战。

[en]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.
它使用来自该质询的服务器nonce，并且第一个客户机nonce值构造A1如下：A1=H(unq(用户名-值)":"unq(realm-value)":"passwd)":"unq(nonce-value)":"unq(cnonce-value)，这为后续请求和响应的认证创建'会话密钥'。这对于每个“认证会话”是不同的，因此限制了任何一个密钥散列的材料量。

[en](Note: see further discussion of the authentication session in Franks, et al.
（注意：参见弗兰克斯等人的认证会话的进一步讨论）。

[en]Standards Track [Page 13] RFC 2617 HTTP Authentication June 1999 section 3.3.) 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.
标准跟踪[第13页]RFC 2617 HTTP认证1999年6月第3.3节)因为服务器仅需要使用用户凭证的散列以创建A1值，所以这种构造可以与第三方认证服务结合使用，使得Web服务器不会需要实际的密码值。

[en]The specification of such a protocol is beyond the scope of this specification.
这种协议的规范超出了本规范的范围。

3.2.2.3 A2

3.2.2.4 Directive values and quoted-string

[en]Note that the value of many of the directives, such as "username- value", are defined as a "quoted-string".
注意，许多指令的值，例如“用户名-值”，被定义为“引用字符串”。

[en]However, the "unq" notation indicates that surrounding quotation marks are removed in forming the string A1.
但是，“UNQ”符号表示在形成字符串A1时删除了周围的引号。

[en]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.
因此，如果授权标头包括字段username="Mufasa"，realm=myhost@testrealm.com，并且用户Mufasa具有密码"Circle of Life"，那么H(A1)将是H(Mufasa:myhost@testrealm.com:Circle of Life)，在摘要的字符串中没有引号。

[en]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.
在应用摘要函数H()的任何字符串中，不允许有空格，除非引用的字符串或实体主体中存在该空格，该实体主体的内容构成要摘要的字符串。

[en]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.
例如，上面所示的字符串A1必须是Mufasa:myhost@testrealm.com:Circle of Life，在冒号的两侧没有空格，但是在密码值中使用的单词之间有空格。

[en]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.
同样地，由H（）所消化的其他字符串在没有任何空白空间的情况下，必须在其每一个界线上都有空白，除非空白空间在引用的字符串或被消化的实体中。

[en]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 Franks, et al.
还要注意，如果应用了完整性保护(qop=auth-int)，H(entity-body)是实体主体的散列，而不是消息主体——它是在发送方Franks等应用任何传输编码之前计算的。

[en]Standards Track [Page 14] RFC 2617 HTTP Authentication June 1999 and after it has been removed by the recipient.
标准跟踪[页面14] RFC 2617 HTTP认证1999年6月和之后它已被收件人删除。

[en]Note that this includes multipart boundaries and embedded headers in each part of any multipart content-type.
请注意，这包括多部分边界和嵌入头在任何多部分内容类型的每个部分中。

3.2.2.5 Various considerations

~~[en]The "Method" value is the HTTP request method as specified in section 5.1.1 of [2].~~
“方法”值是HTTP请求方法，如[5.1]第5.1.1节中所规定的。

~~[en]The "request-uri" value is the Request-URI from the request line as specified in section 5.1.2 of [2].~~
“请求URI”值是请求线中的请求URI，如[5.1]中第5.1.2节所规定的。

~~[en]This may be "*", an "absoluteURL" or an "abs_path" as specified in section 5.1.2 of [2], but it MUST agree with the Request-URI.~~
这可能是“*”、“绝对的URL”或“AbjyPATH”，如[5.1]中的5.1.2节所规定的，但是它必须与请求URI一致。

~~[en]In particular, it MUST be an "absoluteURL" if the Request-URI is an "absoluteURL".~~
特别是，如果请求URI是“绝对URL”，它必须是一个“绝对URL”。

~~[en]The "cnonce-value" is an optional client-chosen value whose purpose is to foil chosen plaintext attacks.~~
“CNOCE值”是一个可选的客户端选择值，其目的是箔选择明文攻击。

~~[en]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.~~
认证服务器必须确保由“URI”指令指定的资源与请求行中指定的资源相同；如果不是，服务器应该返回400个错误请求错误。

~~en 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.~~
（由于这可能是攻击的症状，服务器实现者可能希望考虑记录此类错误。）在该字段中从请求URL复制信息的目的是处理中间代理可能更改客户端请求行的可能性。

~~[en]This altered (but presumably semantically equivalent) request would not result in the same digest as that calculated by the client.~~
这个更改的（但可能在语义上等同）请求不会导致与客户机计算的摘要相同的摘要。

~~[en]Implementers should be aware of how authenticated transactions interact with shared caches.~~
实现者应该知道认证的事务如何与共享高速缓存交互。

~~[en]The HTTP/1.1 protocol specifies that when a shared cache (see section 13.7 of [2]) 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 [2]) directives was present in the response.~~
HTTP/1.1协议规定，当共享高速缓存（参见[2]的第13.7节）接收到包含授权头和中继该请求的响应的请求时，除非两个高速缓存控制（参见第14.9节）中的一个，否则它必须不返回该响应作为对任何其他请求的响应。（2）中的指令存在于响应中。

~~[en]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.~~
如果原始响应包含“.-revalidate”Cache-Control指令，则缓存可能使用该响应的实体来响应后续请求，但是必须首先使用来自新请求的请求头来与原始服务器重新验证该响应，以允许源服务器进行身份验证。提出新的请求。

~~[en]Alternatively, if the original response included the "public" Cache-Control directive, the response entity MAY be returned in reply to any subsequent request.~~
或者，如果原始响应包含“公共”缓存控制指令，则响应于任何后续请求返回响应实体。

3.2.3 The Authentication-Info Header

[en]The Authentication-Info header is used by the server to communicate some information regarding the successful authentication in the response.
服务器使用Authentication-Info头在响应中传递关于成功身份验证的一些信息。

[en]Franks, et al.
弗兰克斯等。

[en]Standards Track [Page 15] RFC 2617 HTTP Authentication June 1999 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 = <"> *LHEX <"> The value of the nextnonce directive is the nonce the server wishes the client to use for a future authentication response.
标准跟踪[第15页]RFC 2617 HTTP身份验证1999年6月AuthenticationInfo="Authentication-Info":"auth-info auth-info=1#(nextnonce|message-qop]|[.-auth]|[cnonce]|[nonce-count])nextnonce="nextnonce-value.-auth="rspauth"="-dige"="-digest响应-digest=<">*LHEX<">nextnonce指令的值是服务器希望客户端用于未来身份验证响应的值。

[en]The server may send the Authentication-Info header with a nextnonce field as a means of implementing one-time or otherwise changing nonces.
服务器可以发送带有nextnonce字段的身份验证信息头部，作为实现一次性或更改nonces的一种方法。

[en]If the nextnonce field is present the client SHOULD use it when constructing the Authorization header for its next request.
如果存在NExtNoCE字段，则客户端在为其下一个请求构造授权标头时应该使用它。

[en]Failure of the client to do so may result in a request to re-authenticate from the server with the "stale=TRUE".
客户端这样做的失败可能导致请求用“STALLE＝true”从服务器重新认证。

[en]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.
服务器实现应该仔细考虑使用这种机制的性能影响；如果每个响应都包括nextnonce指令，则流水线请求是不可能的，nextnonce指令必须用于服务器接收的下一个请求。

[en]Consideration should be given to the performance vs.
应该考虑性能VS。

[en]security tradeoffs of allowing an old nonce value to be used for a limited time to permit request pipelining.
允许旧的临时值用于有限时间以允许请求流水线的安全权衡。

[en]Use of the nonce-count can retain most of the security advantages of a new server nonce without the deleterious affects on pipelining.
使用nonce-count可以保留新服务器nonce的大部分安全优势，而不会对流水线造成有害影响。

[en]message-qop Indicates the "quality of protection" options applied to the response by the server.
消息QOP指示应用于服务器响应的“保护质量”选项。

[en]The value "auth" indicates authentication; the value "auth-int" indicates authentication with integrity protection.
值“AUTH”表示身份验证；值“Authint”表示具有完整性保护的身份验证。

[en]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.
服务器应该在响应中对message-qop指令使用与客户端在对应请求中发送的值相同的值。

[en]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.
“.-auth”指令中可选的响应摘要支持相互验证——服务器证明它知道用户的秘密，并且使用qop=auth-int也提供了对响应的有限完整性保护。

[en]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) Franks, et al.
“响应-摘要”值是针对授权头部中的“请求-摘要”计算的，除非如果“qop=auth”或者在授权头部中没有为请求指定，A2是A2=“:”digest-uri-value，如果“qop=auth-int”，那么A2是A2=“:”digest-uri-value”:“H(实体-主体)”。弗兰克斯等。

[en]Standards Track [Page 16] RFC 2617 HTTP Authentication June 1999 where "digest-uri-value" is the value of the "uri" directive on the Authorization header in the request.
标准跟踪[第16页]RFC 2617 HTTP认证，1999年6月，其中“摘要-uri-value”是请求中授权头上的“uri”指令的值。

[en]The "cnonce-value" and "nc- value" MUST be the ones for the client request to which this message is the response.
“CNOCE值”和“NC-Valk”必须是客户端请求的消息，对此消息是响应。

[en]The "response-auth", "cnonce", and "nonce-count" directives MUST BE present if "qop=auth" or "qop=auth-int" is specified.
如果指定了“QOP= AUTH”或“QOP= AUTINT”，则必须出现“响应AUTH”、“CNONCE”和“NANCE计数”指令。

[en]The Authentication-Info header is allowed in the trailer of an HTTP message transferred via chunked transfer-coding.
在通过分组传输编码传输的HTTP消息的预告片中允许认证信息头。

3.3 Digest Operation

[en]Upon receiving the Authorization header, the server may check its validity by looking up the password that corresponds to the submitted username.
在接收到授权头后，服务器可以通过查找与提交的用户名对应的密码来检查其有效性。

[en]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.
然后，服务器必须执行客户端执行的相同的摘要操作（例如，MD5），并将结果与给定的请求-摘要值进行比较。

[en]Note that the HTTP server does not actually need to know the user's cleartext password.
请注意，HTTP服务器实际上不需要知道用户的明文密码。

[en]As long as H(A1) is available to the server, the validity of an Authorization header may be verified.
只要H（A1）对服务器可用，验证报头的有效性就可以被验证。

[en]The client response to a WWW-Authenticate challenge for a protection space starts an authentication session with that protection space.
客户端对保护空间的WWW-Authenticate质询的响应开始与该保护空间的身份验证会话。

[en]The authentication session lasts until the client receives another WWW-Authenticate challenge from any server in the protection space.
身份验证会话持续到客户端从保护空间中的任何服务器接收到另一个WWW-Authenticate挑战为止。

[en]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.
客户端应该记住与身份验证会话相关联的用户名、密码、nonce、nonce计数和不透明值，以便在该保护空间内的未来请求中构造Authorization头部。

[en]The Authorization header may be included preemptively; doing so improves server efficiency and avoids extra round trips for authentication challenges.
可以先发制人地包括授权头部；这样做可以提高服务器效率并避免验证挑战的额外往返。

[en]The server may choose to accept the old Authorization header information, even though the nonce value included might not be fresh.
服务器可以选择接受旧的授权头信息，即使包含的NoCE值可能不新鲜。

[en]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.
或者，服务器可以用新的NoCe值返回401响应，导致客户端重试请求；通过指定Stay= Trand与此响应，服务器告诉客户端重新尝试新的NoCE，但不提示新用户名和密码。

[en]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.
因为要求客户端在会话期间返回服务器给予它的不透明指令的值，所以不透明数据可以用于传输认证会话状态信息。

en For example, a server could be responsible for authenticating content that actually sits on another server.
（请注意，通过将状态包括在nonce中，还可以更方便和安全地完成任何此类使用。）例如，服务器可以负责对实际位于另一服务器上的内容进行身份验证。

[en]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 Franks, et al.
通过使第一个401响应包括域指令，其值包括第二服务器上的URI，以及不透明指令，其值Franks等，可以实现这一点。

[en]Standards Track [Page 17] RFC 2617 HTTP Authentication June 1999 contains the state information.
标准轨道[页面17] RFC 2617 HTTP认证1999年6月包含状态信息。

[en]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.
客户端将重试该请求，此时服务器可能以301/302重定向来响应，指向第二服务器上的URI。

[en]The client will follow the redirection, and pass an Authorization header , including the data.
客户端将遵循重定向，并通过授权标头，包括<不透明>数据。

[en]As with the basic scheme, proxies must be completely transparent in the Digest access authentication scheme.
与基本方案一样，代理必须在摘要访问认证方案中完全透明。

[en]That is, they must forward the WWW-Authenticate, Authentication-Info and Authorization headers untouched.
也就是说，他们必须转发WWW认证，身份验证信息和授权头未受触动。

[en]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.
如果代理希望在将请求转发到服务器之前对客户端进行身份验证，则可以使用下面3.6节中描述的代理身份验证和代理授权头部来完成。

3.4 Security Protocol Negotiation

~~[en]It is useful for a server to be able to know which security schemes a client is capable of handling.~~
对于服务器来说，能够知道客户端能够处理哪些安全方案是有用的。

~~[en]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.~~
即使服务器不知道客户机支持摘要，服务器也可能希望要求摘要作为其身份验证方法。

~~[en]A client is encouraged to fail gracefully if the server specifies only authentication schemes it cannot handle.~~
如果服务器只指定它无法处理的验证方案，则鼓励客户端优雅地失败。

3.5 Example

[en]The following example assumes that an access-protected document is being requested from the server via a GET request.
下面的示例假定通过GET请求从服务器请求访问受保护的文档。

[en]The URI of the document is "http://www.nowhere.org/dir/index.html".
文档的URI是“http://wwwun.org/dir/index .html”。

[en]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).
客户机和服务器都知道这个文档的用户名是“Mufasa”，密码是“Circle of Life”（三个单词之间各有一个空格）。

[en]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", nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093", opaque="5ccc069c403ebaf9f0171e9517f40e41" The client may prompt the user for the username and password, after which it will respond with a new request, including the following Authorization header: Franks, et al.
客户端第一次请求文档时，没有发送授权头，因此服务器响应：HTTP/1.1 401 Unauthor.WWW-Authenticate:Digest realm="testrealm@host.com"，qop="auth,auth-int"，nonce="dcd98b7102dd2f0dd2f0b11d0f0f600b0b0c093"，opaque="5ccc069c409c403ebaf9f0171e9517f40e41"The客户机可以提示用户输入用户名和密码，之后它将响应新的请求，包括以下授权头：Franks等。

3.6 Proxy-Authentication and Proxy-Authorization

~~[en]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.~~
摘要认证方案还可用于通过使用代理-认证和代理-授权头部来认证用户到代理、代理到代理或到源服务器的代理。

~~[en]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 [2] and their behavior is subject to restrictions described there.~~
这些报头是HTTP/1.1规范[2]第10.33和10.34节中指定的代理身份验证和代理授权报头的实例，并且它们的行为受到此处描述的限制。

~~[en]The transactions for proxy authentication are very similar to those already described.~~
代理验证的事务与已描述的事务非常相似。

~~[en]Upon receiving a request which requires authentication, the proxy/server must issue the "407 Proxy Authentication Required" response with a "Proxy-Authenticate" header.~~
当接收到需要验证的请求时，代理/服务器必须发出“407代理身份验证要求”响应，该响应具有“代理身份验证”头部。

~~[en]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.~~
Proxy-Authenticate报头中使用的摘要挑战与上面3.2.1节中定义的WWW-Authenticate报头的摘要挑战相同。

~~[en]The client/proxy must then re-issue the request with a Proxy- Authorization header, with directives as specified for the Authorization header in section 3.2.2 above.~~
然后，客户端/代理必须用代理授权头重新发出请求，其中使用在上文3.2.2节中为授权头指定的指令。

~~[en]On subsequent responses, the server sends Proxy-Authentication-Info with directives the same as those for the Authentication-Info header field.~~
在随后的响应中，服务器发送带有与Authentication-Info头部字段相同的指令的代理-身份验证-信息。

~~[en]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.~~
请注意，原则上，可以要求客户机同时向代理和终端服务器进行身份验证，但决不能在相同的响应中进行身份验证。

4 Security Considerations

4.1 Authentication of Clients using Basic Authentication

[en]The Basic authentication scheme is not a secure method of user authentication, nor does it in any way protect the entity, which is transmitted in cleartext across the physical network used as the carrier.
基本认证方案不是用户认证的安全方法，也不以任何方式保护实体，该实体以明文形式通过用作载体的物理网络传输。

[en]HTTP does not prevent additional authentication schemes and encryption mechanisms from being employed to increase security or the addition of enhancements (such as schemes to use one-time passwords) to Basic authentication.
HTTP不阻止使用附加的认证方案和加密机制来提高安全性或向基本身份验证添加增强（例如使用一次性密码的方案）。

[en]Franks, et al.
弗兰克斯等。

[en]Standards Track [Page 19] RFC 2617 HTTP Authentication June 1999 The most serious flaw in Basic authentication is that it results in the essentially cleartext transmission of the user's password over the physical network.
标准跟踪[第19页]RFC 2617 HTTP 1999年6月认证基本认证中最严重的缺陷是，它导致用户密码在物理网络上的基本上明文传输。

[en]It is this problem which Digest Authentication attempts to address.
正是这个问题，消化了身份验证试图解决的问题。

[en]Because Basic authentication involves the cleartext transmission of passwords it SHOULD NOT be used (without enhancements) to protect sensitive or valuable information.
因为基本身份验证涉及密码的明文传输，所以不应该使用（没有增强）来保护敏感或有价值的信息。

[en]A common use of Basic authentication is for identification purposes -- requiring the user to provide a user name and password as a means of identification, for example, for purposes of gathering accurate usage statistics on a server.
基本身份验证的一个常见用途是用于标识目的——要求用户提供用户名和密码作为标识手段，例如，用于收集服务器上的准确使用统计信息。

[en]When used in this way it is tempting to think that there is no danger in its use if illicit access to the protected documents is not a major concern.
当以这种方式使用时，如果非法访问受保护的文件不是一个主要问题，那么人们很容易认为使用这种方式没有危险。

[en]This is only correct if the server issues both user name and password to the users and in particular does not allow the user to choose his or her own password.
只有当服务器同时向用户发出用户名和密码并且特别不允许用户选择他或她自己的密码时，这才是正确的。

[en]The danger arises because naive users frequently reuse a single password to avoid the task of maintaining multiple passwords.
危险是因为幼稚的用户频繁重用单个密码以避免维护多个密码的任务。

[en]If a server permits users to select their own passwords, then the threat is not only unauthorized access to documents on the server but also unauthorized access to any other resources on other systems that the user protects with the same password.
如果服务器允许用户选择他们自己的密码，那么威胁不仅是对服务器上的文档的未经授权访问，而且还是对用户使用相同的密码保护的其他系统上的任何其他资源的未经授权访问。

[en]Furthermore, in the server's password database, many of the passwords may also be users' passwords for other sites.
此外，在服务器的密码数据库中，许多密码也可以是其他站点的用户密码。

[en]The owner or administrator of such a system could therefore expose all users of the system to the risk of unauthorized access to all those sites if this information is not maintained in a secure fashion.
因此，如果未以安全的方式维护这些信息，则此类系统的所有者或管理员可能使系统的所有用户面临未经授权访问所有这些站点的风险。

[en]Basic Authentication is also vulnerable to spoofing by counterfeit servers.
基本认证也容易受到伪造服务器的欺骗。

[en]If a user can be led to believe that he is connecting to a host containing information protected by Basic authentication when, in fact, he is connecting to a hostile server or gateway, then the attacker can request a password, store it for later use, and feign an error.
如果当用户连接到恶意服务器或网关时，可以导致用户相信他正在连接到包含受基本身份验证保护的信息的主机，那么攻击者可以请求密码，存储密码供以后使用，并假装错误。

[en]This type of attack is not possible with Digest Authentication.
这种类型的攻击不可能与摘要式身份验证相关联。

[en]Server implementers SHOULD guard against the possibility of this sort of counterfeiting by gateways or CGI scripts.
服务器实现者应该通过网关或CGI脚本来防止这种伪造的可能性。

[en]In particular it is very dangerous for a server to simply turn over a connection to a gateway.
特别是对于服务器来说，简单地将连接切换到网关是非常危险的。

[en]That gateway can then use the persistent connection mechanism to engage in multiple transactions with the client while impersonating the original server in a way that is not detectable by the client.
然后，该网关可以使用持久连接机制与客户机进行多个事务，同时以客户机无法检测到的方式模拟原始服务器。

4.10 Precomputed dictionary attacks

~~[en]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.~~
使用摘要身份验证，如果攻击者可以执行所选择的明文攻击，则攻击者可以将针对许多常见单词的响应预先计算到其选择的临时值，并存储（响应、密码）对的字典。

~~[en]Such precomputation can often be done in parallel on many machines.~~
这种预计算通常可以在许多机器上并行进行。

~~[en]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.~~
然后，它可以使用所选择的明文攻击来获取与该质询对应的响应，并在字典中查找密码。

~~[en]Even if most passwords are not in the dictionary, some might be.~~
即使大多数密码不在字典中，有些可能是。

~~[en]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.~~
由于攻击者可以选择挑战，因此计算列表中每个密码的响应的成本可以与查找许多密码相摊销。

~~[en]A dictionary with 100 million password/response pairs would take about 3.2 gigabytes of disk storage.~~
具有1亿个密码/响应对的字典将占用大约3.2千兆字节的磁盘存储。

~~[en]The countermeasure against this attack is to for clients to be configured to require the use of the optional "cnonce" directive.~~
针对这种攻击的对策是让客户端配置为需要使用可选的“cNONCE”指令。

4.11 Batch brute force attacks

~~[en]With Digest authentication, a MITM can execute a chosen plaintext attack, and can gather responses from many users to the same nonce.~~
使用摘要身份验证，MITM可以执行所选的明文攻击，并且可以收集来自许多用户对同一临时状态的响应。

~~[en]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.~~
然后，它可以在密码空间的任何子集内查找所有密码，这些密码将在该空间上单次传递中生成一个nonce/response对。

~~[en]It also reduces the time to find the first password by a factor equal to the number of nonce/response pairs gathered.~~
它还减少了找到第一个密码的时间等于等于收集的随机数/响应对的数量。

~~[en]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.~~
这种对密码空间的搜索通常可以在许多机器上并行进行，甚至一台机器也能够非常快速地搜索密码空间的大子集——存在这样的报告，即在几个小时内用六个或更少的字母搜索所有密码。

~~[en]The countermeasure against this attack is to for clients to be configured to require the use of the optional "cnonce" directive.~~
针对这种攻击的对策是让客户端配置为需要使用可选的“cNONCE”指令。

4.12 Spoofing by Counterfeit Servers

~~[en]Basic Authentication is vulnerable to spoofing by counterfeit servers.~~
基本认证容易受到伪造服务器的欺骗。

~~[en]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.~~
如果用户能够被引导相信她正在连接到包含由她知道的密码保护的信息的主机，那么当她实际上正在连接到恶意服务器时，恶意服务器可以请求密码，将其存储起来供以后使用，并假装错误。

~~[en]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.~~
使用摘要身份验证时，这种类型的攻击更加困难——但是客户机必须知道需要使用摘要身份验证，可能使用上面描述的一些技术来对付“中间人”攻击。

~~[en]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.~~
同样，通过在解释每个方案的含义时使用适当的指导，对认证机制的视觉指示可以帮助用户检测这种攻击。

~~[en]Franks, et al.~~
弗兰克斯等。

4.13 Storing passwords

[en]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.
摘要身份验证要求身份验证代理（通常是服务器）将从用户名和密码导出的一些数据存储在与给定域相关联的“密码文件”中。

[en]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.
通常，这可能包含由用户名和H(A1)组成的对，其中H(A1)是如上所述的用户名、领域和密码的摘要值。

[en]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.
其安全性含义是，如果此密码文件受到破坏，则攻击者立即使用此域访问服务器上的文档。

[en]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.
与标准的UNIX密码文件不同，不需要解密此信息以便访问与此文件相关联的服务器域中的文档。

[en]On the other hand, decryption, or more likely a brute force attack, would be necessary to obtain the user's password.
另一方面，解密，或更可能是蛮力攻击，将是必要的，以获得用户的密码。

[en]This is the reason that the realm is part of the digested data stored in the password file.
这是因为该域是存储在密码文件中的被消化数据的一部分。

[en]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).
这意味着，如果一个摘要身份验证密码文件被泄露，它不会自动用相同的用户名和密码泄露其他人（尽管它确实使他们受到暴力攻击）。

[en]There are two important security consequences of this.
这有两个重要的安全后果。

[en]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.
首先，密码文件必须受到保护，就好像它包含未加密的密码一样，因为为了访问其域中的文档，它实际上包含未加密的密码。

[en]A second consequence of this is that the realm string should be unique among all realms which any single user is likely to use.
第二个后果是，在任何单个用户都可能使用的所有领域中，领域字符串应该是唯一的。

[en]In particular a realm string should include the name of the host doing the authentication.
特别是，域字符串应该包括进行身份验证的主机的名称。

[en]The inability of the client to authenticate the server is a weakness of Digest Authentication.
客户机无法验证服务器的能力是摘要认证的一个弱点。

4.14 Summary

[en]By modern cryptographic standards Digest Authentication is weak.
通过现代密码标准，摘要认证较弱。

[en]But for a large range of purposes it is valuable as a replacement for Basic Authentication.
但是对于大范围的目的，作为基本认证的替代物是有价值的。

[en]It remedies some, but not all, weaknesses of Basic Authentication.
它弥补了基本认证的一些弱点，但并非所有弱点。

[en]Its strength may vary depending on the implementation.
其强度可能因实施而有所不同。

[en]In particular the structure of the nonce (which is dependent on the server implementation) may affect the ease of mounting a replay attack.
尤其是nonce的结构（这取决于服务器实现）可能会影响安装重放攻击的易用性。

[en]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.
一系列的服务器选项是适当的，因为例如，一些实现可能愿意接受一次性的nonces或摘要的服务器开销，以消除重播的可能性。

[en]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.
其他人可能满足于像上面推荐的仅限于单个IP地址和单个ETag的临时状态，或者满足于有限的生存期。

[en]Franks, et al.
弗兰克斯等。

[en]Standards Track [Page 26] RFC 2617 HTTP Authentication June 1999 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.
标准跟踪[第26页]RFC 2617 HTTP身份验证1999年6月底线是.兼容的实现相对来说比较弱，但.兼容的实现将远远优于基本身份验证。

4.2 Authentication of Clients using Digest Authentication

[en]Digest Authentication does not provide a strong authentication mechanism, when compared to public key based mechanisms, for example.
例如，与基于公钥的机制相比，摘要身份验证不提供强大的身份验证机制。

[en]Franks, et al.
弗兰克斯等。

[en]Standards Track [Page 20] RFC 2617 HTTP Authentication June 1999 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]).
标准跟踪[第20页]RFC 2617 HTTP认证1999年6月，然而，它显著地强于(例如)CRAM-MD5，该CRAM-MD5已经被建议用于LDAP[10]、POP和IMAP(参见RFC 2195[9])。

[en]It is intended to replace the much weaker and even more dangerous Basic mechanism.
它的目的是取代更弱甚至更危险的基本机制。

[en]Digest Authentication offers no confidentiality protection beyond protecting the actual password.
摘要认证在保护实际密码之外不提供机密保护。

[en]All of the rest of the request and response are available to an eavesdropper.
所有其余的请求和响应都可供窃听者使用。

[en]Digest Authentication offers only limited integrity protection for the messages in either direction.
摘要认证仅为消息在任一方向上提供了有限的完整性保护。

[en]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.
如果使用qop=auth-int机制，则在计算WWW-Authenticate和Authorization报头字段响应指令值（参见上面的第3.2节）中使用的消息的那些部分受到保护。

[en]Most header fields and their values could be modified as a part of a man-in-the-middle attack.
大多数头字段和它们的值可以被修改为中间人攻击的一部分。

[en]Many needs for secure HTTP transactions cannot be met by Digest Authentication.
对安全HTTP事务的许多需求不能通过摘要认证来满足。

[en]For those needs TLS or SHTTP are more appropriate protocols.
对于这些需求，TLS或SHTTP是更合适的协议。

[en]In particular Digest authentication cannot be used for any transaction requiring confidentiality protection.
特别是摘要认证不能用于任何需要保密保护的事务。

[en]Nevertheless many functions remain for which Digest authentication is both useful and appropriate.
尽管如此，许多功能仍然适用于摘要式身份验证既有用又适用。

[en]Any service in present use that uses Basic should be switched to Digest as soon as practical.
目前使用BASIC的任何服务都应尽快转换为消化。

4.3 Limited Use Nonce Values

[en]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).
Digest方案使用服务器指定的nonce来对请求摘要值的生成进行种子化（如上面3.2.2.1节中指定的）。

[en]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.
如3.2.1节中的示例nonce所示，服务器可以自由构造nonce，以便它只能从特定客户端、针对特定资源、在有限的时间段或使用次数、或任何其他限制中使用。

[en]Doing so strengthens the protection provided against, for example, replay attacks (see 4.5).
这样做增强了对重放攻击（例如，4.5）所提供的保护。

[en]However, it should be noted that the method chosen for generating and checking the nonce also has performance and resource implications.
然而，应该注意，为生成和检查nonce而选择的方法还具有性能和资源含义。

[en]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.
例如，服务器可以选择只允许使用每个nonce值一次，方法是维护最近发布的每个nonce是否已被返回的记录，并在每个响应的身份验证信息头部字段中发送下一个nonce指令。

[en]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).
这甚至可以防止立即重播攻击，但是检查nonce值成本很高，可能更重要的一点是导致任何流水线请求的认证失败（可能返回过时的nonce指示）。

[en]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.
类似地，合并特定于请求的元素（如用于资源的Etag值）将nonce的使用限制到该版本的资源，并且还会破坏流水线。

[en]Thus it may be useful to do so for methods with side effects but have unacceptable performance for those that do not.
因此，对于副作用的方法可能是有用的，但对于那些不具有副作用的方法可能是不可接受的。

[en]Franks, et al.
弗兰克斯等。

4.4 Comparison of Digest with Basic Authentication

~~[en]Both Digest and Basic Authentication are very much on the weak end of the security strength spectrum.~~
摘要和基本身份验证都是安全强度谱的薄弱环节。

~~[en]But a comparison between the two points out the utility, even necessity, of replacing Basic by Digest.~~
但这两种方法的比较，说明了用文摘代替碱基的必要性、实用性和必要性。

~~[en]The greatest threat to the type of transactions for which these protocols are used is network snooping.~~
使用这些协议的事务类型的最大威胁是网络窥探。

~~[en]This kind of transaction might involve, for example, online access to a database whose use is restricted to paying subscribers.~~
这种事务可能涉及，例如，在线访问一个数据库，该数据库的使用仅限于付费用户。

~~[en]With Basic authentication an eavesdropper can obtain the password of the user.~~
通过基本身份验证，窃听者可以获得用户的密码。

~~[en]This not only permits him to access anything in the database, but, often worse, will permit access to anything else the user protects with the same password.~~
这不仅允许他访问数据库中的任何内容，而且更糟糕的是，将允许访问用户使用相同密码保护的其他内容。

~~[en]By contrast, with Digest Authentication the eavesdropper only gets access to the transaction in question and not to the user's password.~~
相比之下，使用摘要身份验证，窃听者只能访问所讨论的事务，而不能访问用户的密码。

~~[en]The information gained by the eavesdropper would permit a replay attack, but only with a request for the same document, and even that may be limited by the server's choice of nonce.~~
窃听者获得的信息将允许重放攻击，但是仅允许对同一文档的请求，甚至可能受到服务器选择nonce的限制。

4.5 Replay Attacks

[en]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.
对于简单的GET请求，针对Digest身份验证的重放攻击通常是毫无意义的，因为窃听者已经看到了通过重放可以获得的唯一文档。

[en]This is because the URI of the requested document is digested in the client request and the server will only deliver that document.
这是因为所请求的文档的URI在客户机请求中被摘要，并且服务器将只传递该文档。

[en]By contrast under Basic Authentication once the eavesdropper has the user's password, any document protected by that password is open to him.
相比之下，在Basic Authentication下，一旦窃听者拥有了用户的密码，则受该密码保护的任何文档都将对他开放。

[en]Thus, for some purposes, it is necessary to protect against replay attacks.
因此，出于某些目的，有必要防止重放攻击。

[en]A good Digest implementation can do this in various ways.
一个好的摘要实现可以通过各种方式来实现。

[en]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.
服务器创建的“nonce”值依赖于实现，但是如果它包含客户端IP的摘要、时间戳、资源ETag和私有服务器密钥（如上面推荐的），那么重放攻击就不简单。

[en]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.
攻击者必须使服务器确信请求来自错误的IP地址，并且必须使服务器将文档传递到与其认为正在向其发送文档的地址不同的IP地址。

[en]An attack can only succeed in the period before the time-stamp expires.
攻击只能在时间戳到期之前的一段时间内成功。

[en]Digesting the client IP and time-stamp in the nonce permits an implementation which does not maintain state between transactions.
在NoCE中消化客户端IP和时间戳允许在事务之间不保持状态的实现。

[en]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.
对于不能容忍重放攻击的应用程序，服务器可以使用一次性的临时值，该值不会被允许第二次使用。

[en]This requires the overhead of the server Franks, et al.
这需要服务器弗兰克斯等的开销。

[en]Standards Track [Page 22] RFC 2617 HTTP Authentication June 1999 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.
标准跟踪[第22页]RFC 2617 HTTP认证，1999年6月，记住使用哪个nonce值直到nonce时间戳（以及由此构建的摘要）过期，但它有效地防止重放攻击。

[en]An implementation must give special attention to the possibility of replay attacks with POST and PUT requests.
实现必须特别注意使用POST和PUT请求进行重放攻击的可能性。

~~[en]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.~~
除非服务器使用一次性或限制性使用nonces和/或坚持使用qop=auth-int的完整性保护，否则攻击者可以用伪造表单数据或其他消息体重放来自成功请求的有效凭证。

~~[en]Even with the use of integrity protection most metadata in header fields is not protected.~~
即使使用完整性保护，头字段中的大多数元数据也不受保护。

~~[en]Proper nonce generation and checking provides some protection against replay of previously used valid credentials, but see 4.8.~~
正确的NoCe生成和检查提供了一些防止先前使用的有效凭据重放的保护，但是请参见4.8。

4.6 Weakness Created by Multiple Authentication Schemes

~~[en]An HTTP/1.1 server may return multiple challenges with a 401 (Authenticate) response, and each challenge may use a different auth-scheme.~~
HTTP/1.1服务器可以返回具有401(Authenticate)响应的多个挑战，并且每个挑战可以使用不同的认证方案。

~~[en]A user agent MUST choose to use the strongest auth-scheme it understands and request credentials from the user based upon that challenge.~~
用户代理必须选择使用它所理解的最强的AUTH方案，并根据该请求向用户请求凭据。

~~[en]Note that many browsers will only recognize Basic and will require that it be the first auth-scheme presented.~~
注意，许多浏览器只会识别BASIC，并要求它是第一个AUTH方案。

~~[en]Servers should only include Basic if it is minimally acceptable.~~
如果最低限度的接受，服务器应该只包括BASIC。

~~[en]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.~~
当服务器使用WWW-Authenticate报头提供认证方案的选择时，所得到的认证的强度仅与最弱的认证方案的强度一样好。

~~[en]See section 4.8 below for discussion of particular attack scenarios that exploit multiple authentication schemes.~~
参见下面的第4.8节讨论利用多个验证方案的特定攻击场景。

4.7 Online dictionary attacks

~~[en]If the attacker can eavesdrop, then it can test any overheard nonce/response pairs against a list of common words.~~
如果攻击者可以窃听，那么它可以测试任何窃听的随机/响应对一个共同的单词列表。

~~[en]Such a list is usually much smaller than the total number of possible passwords.~~
这样的列表通常比可能的密码的总数小得多。

~~[en]The cost of computing the response for each password on the list is paid once for each challenge.~~
计算每一个密码在列表上的响应的费用为每个挑战支付一次。

~~[en]The server can mitigate this attack by not allowing users to select passwords that are in a dictionary.~~
服务器可以通过不允许用户选择字典中的密码来减轻这种攻击。

~~[en]Franks, et al.~~
弗兰克斯等。

4.8 Man in the Middle

[en]Both Basic and Digest authentication are vulnerable to "man in the middle" (MITM) attacks, for example, from a hostile or compromised proxy.
基本身份验证和摘要身份验证都容易受到“中间人”（MITM）攻击，例如，来自恶意或受损的代理的攻击。

[en]Clearly, this would present all the problems of eavesdropping.
显然，这会引起窃听的所有问题。

[en]But it also offers some additional opportunities to the attacker.
但它也给攻击者提供了一些额外的机会。

[en]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.
可能的中间人攻击是将弱身份验证方案添加到选项集，希望客户端将使用公开用户凭证的方案（例如：

[en]password).
密码）。

[en]For this reason, the client should always use the strongest scheme that it understands from the choices offered.
由于这个原因，客户端应该总是使用从所提供的选择中理解的最强的方案。

[en]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.
更好的MITM攻击是删除所有提供的选项，代之以仅请求基本身份验证的挑战，然后使用来自基本身份验证的明文凭证使用其请求的更强方案向源服务器进行身份验证。

[en]A particularly insidious way to mount such a MITM attack would be to offer a "free" proxy caching service to gullible users.
安装这种MITM攻击的一种特别阴险的方法是为易受欺骗的用户提供免费的代理缓存服务。

[en]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.
用户代理应该考虑诸如在凭证请求时呈现要使用什么认证方案的可视指示之类的措施，或者记住服务器请求过的最强认证方案，并在使用较弱的认证方案之前产生警告消息。

[en]It might also be a good idea for the user agent to be configured to demand Digest authentication in general, or from specific sites.
对于用户代理来说，最好配置成要求摘要身份验证，或者从特定站点进行身份验证。

[en]Or, a hostile proxy might spoof the client into making a request the attacker wanted rather than one the client wanted.
或者，恶意的代理可能会欺骗客户端请求攻击者的请求，而不是客户端想要的请求。

[en]Of course, this is still much harder than a comparable attack against Basic Authentication.
当然，这仍然比对基本身份验证的攻击更困难。

4.9 Chosen plaintext attacks

~~[en]With Digest authentication, a MITM or a malicious server can arbitrarily choose the nonce that the client will use to compute the response.~~
使用摘要身份验证，MITM或恶意服务器可以任意选择客户端将用于计算响应的nonce。

~~[en]This is called a "chosen plaintext" attack.~~
这被称为“选择明文”攻击。

~~[en]The ability to choose the nonce is known to make cryptanalysis much easier [8].~~
已知选择NoCE的能力使密码分析变得更容易[8]。

~~[en]However, no way to analyze the MD5 one-way function used by Digest using chosen plaintext is currently known.~~
然而，目前无法知道使用选择明文来分析摘要所使用的MD5单向函数。

~~[en]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.~~
针对这种攻击的对策是客户端被配置为需要使用可选的“cNONCE”指令；这允许客户端以攻击者未选择的方式改变对哈希的输入。

~~[en]Franks, et al.~~
弗兰克斯等。

5 Sample implementation

[en]The following code implements the calculations of H(A1), H(A2), request-digest and response-digest, and a test program which computes the values used in the example of section 3.5.
下面的代码实现了H(A1)、H(A2)、请求-摘要和响应-摘要的计算，以及计算3.5节示例中使用的值的测试程序。

[en]It uses the MD5 implementation from RFC 1321.
它使用来自RFC 1321的MD5实现。

[en]File "digcalc.h": #define HASHLEN 16 typedef char HASH[HASHLEN]; #define HASHHEXLEN 32 typedef char HASHHEX[HASHHEXLEN+1]; #define IN #define OUT / *calculate H(A1) as per HTTP Digest spec* / void DigestCalcHA1(IN char *pszAlg, IN char* pszUserName, IN char *pszRealm, IN char* pszPassword, IN char *pszNonce, IN char* pszCNonce, OUT HASHHEX SessionKey); / *calculate request-digest/response-digest as per HTTP Digest spec* / void DigestCalcResponse(IN HASHHEX HA1, / *H(A1)* / IN char *pszNonce, /* nonce from server */ *IN char* pszNonceCount, / *8 hex digits* / IN char *pszCNonce, /* client nonce */ *IN char* pszQop, / *qop-value: "", "auth", "auth-int"* / IN char *pszMethod, /* method from the request */ *IN char* pszDigestUri, / *requested URL* / IN HASHHEX HEntity, / *H(entity body) if qop="auth-int"* / OUT HASHHEX Response / *request-digest or response-digest* /); File "digcalc.c": #include #include Franks, et al.
文件“DigCalc.h”：定义HhhLLN 16 TyPulf chhash（hhhLLeN）；定义*HasHexLeN 32 TyPulfCar hhhEx [HasHexLeN + 1]*；*y*定义为*OUT/***计算*h*（*A1*），按*http*摘要规格/空格*DigestCalch1*（在*char* PSZalg中，在char *PSZUrNeX*中，在*char* PSZEnter中，以char *PSZCOMPION*，*inchar* PSZNONCE，在char *PSZCNONCE*中，输出*HASHHEX SessionKey*）；/按HTTP摘要规格/空格DigestCalcResponse计算请求摘要/响应摘要（在HashEX HA1中，/*H*（*A1*）/在char *PSZNONCE*中，/NoCE来自服务器/*char* PSZNONECECUT，/ *8*十六进制数字//在char *PSZCNNOCE*中，/客户端NoCy//char *PSZQOP*，/QOP值：“”，“AUTH”，“Authint”/*在char* PSZ方法，/方法从请求/char *PSZigestururi*，/请求URL/*HasHEX-HEnt*实体，/H（实体体），如果QOP＝“Authint”/*Out-HasHeX*响应/请求摘要或响应摘要*/）；DigCalc.C：：包括< Global，H>α，包括MD5.H.弗兰克斯等。

[en]Standards Track [Page 27] RFC 2617 HTTP Authentication June 1999 #include #include "digcalc.h" void CvtHex(IN HASH Bin, OUT HASHHEX Hex) { unsigned short i; unsigned char j; for (i = 0; i < HASHLEN; i++) { j = (Bin[i] >> 4) & 0xf; if (j <= 9) Hex[i*2] = (j + '0'); else Hex[i*2] = (j + 'a' - 10); j = Bin[i] & 0xf; if (j <= 9) Hex[i2*+1] = (j + '0'); else Hex[i*2+1] = (j + 'a' - 10); }; Hex[HASHHEXLEN] = '\0'; }; / *calculate H(A1) as per spec* / void DigestCalcHA1(IN char *pszAlg, IN char* pszUserName, IN char *pszRealm, IN char* pszPassword, IN char *pszNonce, IN char* pszCNonce, OUT HASHHEX SessionKey) { MD5_CTX Md5Ctx; HASH HA1; MD5Init(&Md5Ctx); MD5Update(&Md5Ctx, pszUserName, strlen(pszUserName)); MD5Update(&Md5Ctx, ":", 1); MD5Update(&Md5Ctx, pszRealm, strlen(pszRealm)); MD5Update(&Md5Ctx, ":", 1); MD5Update(&Md5Ctx, pszPassword, strlen(pszPassword)); MD5Final(HA1, &Md5Ctx); if (strıcmp(pszAlg, "md5-sess") == 0) { Franks, et al.
标准轨道[第27页]RFC 2617HTTP认证1999年6月..#包括.<字符串.h>..#包括.<字符串.h>.#包括"digcalc.h "digcalc.h"空CvtHex (在HASH宾，OUHASHHEHEHEX六，OUT HASHHEX六六六六六(IN HASH宾宾，OUT HASHHEX六，OUHASHHEX六六)中){无符号短i；无符号字符j;无符号字符j j；用于(i=0;i=0;i；i；i<HASHLELEN；i<0；i<HASHLELELEN；i<HASHLEN；i<HASHLEN；i<HASHLENi；i；i+++[*i2]=(j+)'a'-10)；j=Bin[i]&0xf;*如果*(j<=9)Hex[i'22+1]=(j++1] =_(j++0'+1]=(j+22+1]]]=(j+2+1 1](j+1+1*；}；
Hex[HASHHEHEXHEHEHEHEXLEXLELEN]]=.'\\0'; ; ; }}；/计算*H(A1)*根据具体/voidDigestCalCalcCalcCalcCACACACACACACACCACACACACACACACACACACACACACACACACACACACACACACACACACACACACACACACpszPas.，IN char*pszNonce*，*IN char*psOUT HASHHEX SessionKey){MD5_CTX Md5Ctx；HASH HA1；MD5Init（&Md5Ctx）；MD5Update（&Md5Ctx，psz用户名，strlen（pszUse用户名，str用户名）MD5Update（&Md5Ctx，psz用户名，strlen（&Md5Ctx，pszUseUser用户名，strlen（pszReareaXXXXXXXXXXXXXXXMd5Md5Ctx，pszRealm，pszRealm，strlen（pszRearealm））））；MD5Update（&Md5Update（&Md5Ctx&Md5Ctx(&Md5Ctx、pszPas.、strlen(pszPas.))；MD5FinaL（HA1和MD5CTX）；IF（StRMP（PSZALG，MD5 SESS）＝＝0）{弗兰克斯等。

[en]Standards Track [Page 28] RFC 2617 HTTP Authentication June 1999 MD5Init(&Md5Ctx); MD5Update(&Md5Ctx, HA1, HASHLEN); MD5Update(&Md5Ctx, ":", 1); MD5Update(&Md5Ctx, pszNonce, strlen(pszNonce)); MD5Update(&Md5Ctx, ":", 1); MD5Update(&Md5Ctx, pszCNonce, strlen(pszCNonce)); MD5Final(HA1, &Md5Ctx); }; CvtHex(HA1, SessionKey); }; /* *calculate request-digest/response-digest as per HTTP Digest spec* */ void DigestCalcResponse(IN HASHHEX HA1, /* *H(A1)* */ IN char *pszNonce,* /* nonce from server */ *IN char* pszNonceCount, /* *8 hex digits* */ IN char *pszCNonce,* /* client nonce */ *IN char* pszQop, /* *qop-value: "", "auth", "auth-int"* */ IN char *pszMethod,* /* method from the request */ *IN char* pszDigestUri, /* *requested URL* */ IN HASHHEX HEntity, /* *H(entity body) if qop="auth-int"* */ OUT HASHHEX Response /* *request-digest or response-digest* */) { MD5_CTX Md5Ctx; HASH HA2; HASH RespHash; HASHHEX HA2Hex; // calculate H(A2) MD5Init(&Md5Ctx); MD5Update(&Md5Ctx, pszMethod, strlen(pszMethod)); MD5Update(&Md5Ctx, ":", 1); MD5Update(&Md5Ctx, pszDigestUri, strlen(pszDigestUri)); if (strcmp(pszQop, "auth-int") == 0) { MD5Update(&Md5Ctx, ":", 1); MD5Update(&Md5Ctx, HEntity, HASHHEXLEN); }; MD5Final(HA2, &Md5Ctx); CvtHex(HA2, HA2Hex); // calculate response MD5Init(&Md5Ctx); MD5Update(&Md5Ctx, HA1, HASHHEXLEN); MD5Update(&Md5Ctx, ":", 1); MD5Update(&Md5Ctx, pszNonce, strlen(pszNonce)); MD5Update(&Md5Ctx, ":", 1); if (*pszQop) { Franks, et al.
标准跟踪[第28页]RFC 2617HTTP认证；1999年6月；MD5更新（&Md5Ctx，HA1，HASHLEN）；MD5更新（&Md5Ctx，HA1，HASHLEN）；MD5更新（&Md5Ctx，&Md5Ctx，pszNonce，strlen（pszNonNonce）；MD5更新（&Md5Ctx，&Md5Ctx，&Md5Ctx，&Md5Ctx，pszCNctx，pszCN.，strlen（pszCNCNCN一次））；MD55Fin5FinFin5FinMD5Fin5Fin555FinXXXx，MD5FinMD5CNCNCNCNCNCNCNCNMDMDMDMDMDMDMD5al(HA1,&Md5Ctx);};CvtHex(HA1，SessionKey)；}；/根据*HTTP*摘要规范/void DigestCalcResponse(IN HASHHEX HA1，/*H(A1)*/IN char*pszNonce*，/nonce from server*/IN char*pszNonceCount，/*8hex digits*/IN char*pszCN.*，/client nonce*/IN char*pszQop，/*client nonce*/IN char*pszQop*，/qop-value:“”、“auth”、“auth-int”*/IN char*psz., /来自*request*/IN char*pszDigestUri*的方法, /requested URL*/IN HASHHEX HEntity, /*H(实体主体)，如果qop=“auth-int”*/OUT HASHHEX Response/*request-digest或.-digest*/){MD5_CTX Md5Ctx;HASH HASH HA2;HASH RespHash;H计算H(A2)MD5Init(&Md5Ctx)；{MD5Update(&Md5Ctx，psz.，strlen(psz.))；MD5Update(&Md5Ctx(&Md5Ctx(&Md5Ctx，“：：：：1”)；MD5Update(&Md5Ctx(&Md5Ctx(&Md5Ctx，“：：：：：1)；MD5Update(&Md5Ctx&Md5Ctx，&Md5Ctx，&Md5Ctx，“：：：：：：：：：：：：：：：；；；；；；；；；；；；；；MD5Update(&Md5Update(MD5Update(&Md5Ctx,HEntity,HASHHEXLEN);};D5Final(HA2,&Md5Ctx);CvtHex(HA2,HA2Hex);//计算响应MD5Init(&Md5Ctx(&Md5Ctx,HA1,HASHHEXLEN)；MD5Update(&Md5Ctx,HA2,&Md5Ctx;Ctx(HA2,HA2Hex)；//计算响应MD5更新MD5Init(&Md5Init(&Md5Ctx,HA5Ctx&Md5Ctx,&Md5Ctx)；//Md5Ctx;Md5Ctx;MD5计算计算响应MD5Md5Md5Ctx(&Md5Ctx(&Md5Ct等人。

[en]Standards Track [Page 29] RFC 2617 HTTP Authentication June 1999 MD5Update(&Md5Ctx, pszNonceCount, strlen(pszNonceCount)); MD5Update(&Md5Ctx, ":", 1); MD5Update(&Md5Ctx, pszCNonce, strlen(pszCNonce)); MD5Update(&Md5Ctx, ":", 1); MD5Update(&Md5Ctx, pszQop, strlen(pszQop)); MD5Update(&Md5Ctx, ":", 1); }; MD5Update(&Md5Ctx, HA2Hex, HASHHEXLEN); MD5Final(RespHash, &Md5Ctx); CvtHex(RespHash, Response); }; File "digtest.c": #include #include "digcalc.h" void main(int argc, char ** argv) { char* pszNonce = "dcd98b7102dd2f0e8b11d0f600bfb0c093"; char *pszCNonce = "0a4f113b"; char* pszUser = "Mufasa"; char *pszRealm = "testrealm@host.com"; char* pszPass = "Circle Of Life"; char *pszAlg = "md5"; char szNonceCount[9] = "00000001"; char* pszMethod = "GET"; char *pszQop = "auth"; char* pszURI = "/dir/index.html"; HASHHEX HA1; HASHHEX HA2 = ""; HASHHEX Response; DigestCalcHA1(pszAlg, pszUser, pszRealm, pszPass, pszNonce, pszCNonce, HA1); DigestCalcResponse(HA1, pszNonce, szNonceCount, pszCNonce, pszQop, pszMethod, pszURI, HA2, Response); printf("Response = %s\n", Response); }; Franks, et al.
标准跟踪[第29页]RFC 2617HTTP认证1999年6月MD5更新(&Md5Ctx，pszNonce计数，strlen(pszNonce计数)MD5更新(&Md5Ctx，pszNonce计数，strlen(pszNo4141414141414141414141414141CNCNCNCNCN.))；MD5更新(&Md5Ctx，psz5Ctx，psz5Ctx，pszQop，strlen(pszQop))；MD5更新更新(&Md5更新更新(&Md55更新号，pszQop，pszQop(pszQop(pszQQop))；MD5更新MD5更新MD5更新MD5更新MD5更新日期(&Md5Ctx, ":",1)}；MD5Update(&Md5Ctx，HA2Hex，HASHHEXLEN)；MD5最终(RespHash，&Md5Ctx)；CvtHex(RespHash，响应)；}；文件“digtest.c”；}；文件“digtest.c”：#包括#包括“digcalc.h”void main(int argc，char**argv**argv){char*pszNonce="char*pszNonce="dcd98b7102022d7122222222222626262626262626262626262626262626262626262626

26262626262626262626262222f2f0f83;char*pszCN.="0a4f113b"*；*char*psz.r =Mufasa；char*pszRealm= "char*pszRealm= "testrealm@host.com；char*pszPass= "生命圈"*；
*char*pszPass="Tesfasa;char*char*pszRealm="testreasa@char;char*char*pszRealm;char*char*char*pszRearearearearealm ="testreasa@host@host.com.com;char*pszPaszRearearearearearearealm="testreasafadoreasafafasafasasasasas asasasasasasasasasasasasasasasasasasasasasasasasasasasasasasasasasasasasasaDigestCalcHA1(pszA)lg 、pszUser、pszRealm、pszPass、pszNonce、pszCN.、HA1；DigestCalcResponse(HA1、pszNonce、szNonceCount、pszCN.、pszQop、psz.、pszURI、HA2、Response)；printf("Response=%sn"，Response)；}；Franks等。

6 Acknowledgments

~~[en]Eric W.~~
埃里克W

~~[en]Sink, of AbiSource, Inc., was one of the original authors before the specification underwent substantial revision.~~
AbISOURCE公司的Sink，是在规范进行了实质性修订之前的原作者之一。

~~[en]In addition to the authors, valuable discussion instrumental in creating this document has come from Peter J.~~
除了作者之外，有助于创建该文档的有价值的讨论来自Peter J.。

~~[en]Churchyard, Ned Freed, and David M.~~
教堂墓地，奈德·弗莱德和David M.

~~[en]Kristol.~~
克里斯托。

~~[en]Jim Gettys and Larry Masinter edited this document for update.~~
Jim Gettys和Larry Masinter编辑了这份文件进行更新。

7 References

~~[en][1] Berners-Lee, T., Fielding, R.~~
〔1〕Berners Lee、T.、菲尔丁、R.

~~[en]and H.~~
H.

~~[en]Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0", RFC 1945, May 1996.~~
FryStuk，“超文本传输协议-HTTP / 1”，RFC 1945，1996年5月。

~~[en][2] Fielding, R., Gettys, J., Mogul, J., Frysyk, H., Masinter, L., Leach, P.~~
〔2〕菲尔丁，R，Gettys，J.，MuGul，J.，FrySyk，H，MasTalm，L.，LeCh，P.

~~[en]and T.~~
和T。

~~[en]Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.~~
Berners Lee，“超文本传输协议--HTTP / 1.1”，RFC 2616，1999年6月。

~~[en][3] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.~~
（3）RiestR.，R，“MD5消息摘要算法”，RFC 1321，1992年4月。

~~[en][4] Freed, N.~~
（4）解放了，N.

~~[en]and N.~~
N.

~~[en]Borenstein.~~
博伦斯坦。

~~[en]"Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.~~
“多用途因特网邮件扩展（MIME）：第一部分：因特网消息体的格式”，RFC 2045，1996年11月。

~~[en][5] Dierks, T.~~
〔5〕迪尔克斯，T。

~~[en]and C.~~
C.

~~[en]Allen "The TLS Protocol, Version 1.0", RFC 2246, January 1999.~~
艾伦“TLS协议，版本1”，RFC 2246，1999年1月。

~~[en][6] Franks, J., Hallam-Baker, P., Hostetler, J., Leach, P., Luotonen, A., Sink, E.~~
〔6〕弗兰克斯、J.、哈勒姆·贝克、P、主持人、J.、利奇、P、Luotonen、A、Sink、E.

~~[en]and L.~~
L.

~~[en]Stewart, "An Extension to HTTP : Digest Access Authentication", RFC 2069, January 1997.~~
斯图尔特，“对HTTP的扩展：摘要访问认证”，RFC 2069，1997年1月。

~~[en][7] Berners-Lee, T, Fielding, R.~~
〔7〕Berners Lee，T，菲尔丁，R.

[en]and L.
L.

[en]Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.
MASSIN，“统一资源标识符（URI）：通用语法”，RFC 2396，1998年8月。

[en][8] Kaliski, B.,Robshaw, M., "Message Authentication with MD5", CryptoBytes, Sping 1995, RSA Inc, (http://www.rsa.com/rsalabs/pubs/cryptobytes/spring95/md5.htm) [9] Klensin, J., Catoe, R.
[8]Kaliski，B.，Robshaw，M.，“用MD5进行消息认证”，CryptoBytes，Sping 1995，RSA公司，(http://www.rsa.com/rsalabs/pubs/cryptobytes/spring95/md5.htm)[9]Klensin，J.，Catoe，R.

[en]and P.
P.

[en]Krumviede, "IMAP/POP AUTHorize Extension for Simple Challenge/Response", RFC 2195, September 1997.
KrimVIEDE，“IMAP/POP授权扩展为简单的挑战/响应”，RFC 2195，1997年9月。

[en][10] Morgan, B., Alvestrand, H., Hodges, J., Wahl, M., "Authentication Methods for LDAP", Work in Progress.
〔10〕摩根，B，PothStudio，H，霍奇，J.，瓦尔，M，“LDAP的认证方法”，正在进行中。

[en]Franks, et al.
弗兰克斯等。

8 Authors' Addresses

[en]John Franks Professor of Mathematics Department of Mathematics Northwestern University Evanston, IL 60208-2730, USA EMail: john@math.nwu.edu Phillip M.
约翰·弗兰克斯，西北大学埃文斯顿数学系教授，IL 60208-2730，美国电子邮件：John@math.nwu.edu Phillip M.

[en]Hallam-Baker Principal Consultant Verisign Inc.
哈勒姆贝克首席顾问VrISIGN公司

[en]301 Edgewater Place Suite 210 Wakefield MA 01880, USA EMail: pbaker@verisign.com Jeffery L.
301 EdgWew地方套房210 Wekfield马01880，美国电子邮件：Pakel@ VISISIGN Jeffery L.

[en]Hostetler Software Craftsman AbiSource, Inc.
HooTeTror软件工匠AbasurCE公司

[en]6 Dunlap Court Savoy, IL 61874 EMail: jeff@AbiSource.com Scott D.
6邓拉普法院萨沃伊，IL 61874电子邮件：JFEH-ABISURCEC.com Scott D.

[en]Lawrence Agranat Systems, Inc.
劳伦斯阿格拉纳特系统公司

[en]5 Clocktower Place, Suite 400 Maynard, MA 01754, USA EMail: lawrence@agranat.com Paul J.
5钟楼广场，套房400，梅纳德，马01754，美国电子邮件：劳伦斯@ AgRANTAT.com Paul J.

[en]Leach Microsoft Corporation 1 Microsoft Way Redmond, WA 98052, USA EMail: paulle@microsoft.com Franks, et al.
利奇微软公司1微软RADMDEN，WA 98052，美国电子邮件：Paulle @微软公司弗兰克斯等。

[en]Standards Track [Page 32] RFC 2617 HTTP Authentication June 1999 Ari Luotonen Member of Technical Staff Netscape Communications Corporation 501 East Middlefield Road Mountain View, CA 94043, USA Lawrence C.
标准轨道[第32页]RFC 2617HTTP认证1999年6月美国劳伦斯C.

[en]Stewart Open Market, Inc.
斯图尔特公开市场公司

[en]215 First Street Cambridge, MA 02142, USA EMail: stewart@OpenMarket.com Franks, et al.
215第一街剑桥，马02142，美国电子邮件：StWurt@ OpenSalmCo弗兰克斯，等。

9. Full Copyright Statement