本附录包含了实现 HTTP 摘要认证功能所需的支撑数据和源代码。

F.1 摘要WWW-Authenticate指令

表 F-1 根据 RFC 2617 中的描述，对 WWW-Authenticate 指令进行了说明。与往常一样，最新细节请参见官方规范。

表F-1 （来自RFC 2617的）摘要WWW-Authenticate首部指令

指　令	描　述
realm	显示给用户的字符串，这样用户就可以知道该使用哪个用户名和密码了。这个字符串中至少应该包含执行认证功能的主机名字，此外可能还会说明可能拥有访问权的用户的集合。例如，registered_users@gotham.news.com
nonce	服务器特有的数据字符串，每次产生一个 401 响应时都应该生成一个唯一的数据字符串。建议这个字符串为 Base-64 或十六进制数据。需要特别说明的是，由于此字符串是放在首部行中作为引用字符串传送的，所以不允许使用双引号。 nonce 的内容是与实现有关的。实现的质量取决于选择是否合适。比如，可以将 nonce 构造成以下内容的 Base-64 编码： `time-stamp H(time-stamp ":" ETag ":" private-key)` 其中 time-stamp 是服务器生成的时间或其他不重复的数值，ETag 是与所请求实体有关的 HTTP ETag 首部的值，private-key 是只有服务器知道的数据。使用这种形式的 nonce，服务器会在收到客户端的 Authentication 首部之后重新对散列部分进行计算，如果与该首部的 nonce 不符，或者时间戳的值不够近，就可以拒绝请求。通过这种方式，服务器可以限制 nonce 的有效时间。包含 ETag 可以防止对资源更新版本的重放请求。（注意：在 nonce 中包含客户端的 IP 地址，看起来好像为服务器提供了限制最初获得此 nonce 的客户端重用 nonce 的能力，但这样会破坏代理集群，来自单个用户的请求通常都会经过集群中不同的代理进行传输。而且，IP 地址欺骗也不是很难。） 实现可以选择不接受以前用过的 nonce，或以前用过的摘要，以防止重放攻击，或者选择为 POST 或 PUT 请求使用一次性 nonce 或摘要，为 GET 请求使用时间戳
domain	一个引用的、由空格分隔的 URI 列表（如 RFC 2396，“Uniform Resource Identifiers: GenericSyntax”所述），这些 URI 定义了保护空间。如果 URI 是个 abs_path，它就是相对于受访服务器的典型根 URL 的。这个列表中的绝对 URI 所指的服务器可能不是受访服务器。 客户端可以用这个列表来判定应该将同样的认证信息发送给哪个 URI 集：可以假定所有以此列表中的 URI 作为前缀的 URI（在将两者都转换为绝对 URI 之后）都位于同一个保护空间内。 如果省略了这条指令，或者其值为空，客户端就应该假定保护空间中包含了响应服务器上的所有 URI。 这条指令在 Proxy-Authenticate 首部是无意义的，此时，保护空间总是包括整个代理；如果提供了这条指令，也应该将其忽略

574