基本认证便捷灵活，但极不安全。用户名和密码都是以明文形式传送的，[1]也没有采取任何措施防止对报文的篡改。安全使用基本认证的唯一方式就是将其与 SSL 配合使用。

摘要认证与基本认证兼容，但却更为安全。本章主要介绍摘要认证的原理和实际应用。尽管摘要认证还没有得到广泛应用，但对实现安全事务来说，这些概念是非常重要的。

13.1 摘要认证的改进

摘要认证是另一种 HTTP 认证协议，它试图修复基本认证协议的严重缺陷。具体来说，摘要认证进行了如下改进。

- 永远不会以明文方式在网络上发送密码。
- 可以防止恶意用户捕获并重放认证的握手过程。
- 可以有选择地防止对报文内容的篡改。
- 防范其他几种常见的攻击方式。

摘要认证并不是最安全的协议。[2]摘要认证并不能满足安全 HTTP 事务的很多需求。对这些需求来说，使用传输层安全（Transport Layer Security，TLS）和安全 HTTP
286 （Secure HTTP，HTTPS）协议更为合适一些。

但摘要认证比它要取代的基本认证强大很多。与很多建议其他因特网服务使用的常用策略相比，（比如曾建议 LDAP、POP 和 IMAP 使用的 CRAM-MD5），摘要认证也要强大很多。

迄今为止，摘要认证还没有被广泛应用。但由于基本认证存在固有的安全风险，HTTP 设计者曾在 RFC 2617 中建议："在可行的情况下应该将目前在用的所有使用基本认证的服务，尽快地转换为摘要认证方式。"[3]这个标准的前景还不太明朗。

13.1.1 用摘要保护密码

摘要认证遵循的箴言是"绝不通过网络发送密码"。客户端不会发送密码，而是会发送一个"指纹"或密码的"摘要"，这是密码的不可逆扰码。客户端和服务器都知道这个密码，因此服务器可以验证所提供的摘要是否与密码相匹配。只拿到摘要的话，除了将所有的密码都拿来试试之外，没有其他方法可以找出摘要是来自哪个密

注 1：用户名和密码用 Base-64 编码进行了扰码，但很容易被解码。只能防止无意中的查看，没有任何防止恶意用户攻击的手段。

注 2：比如，与基于公有密钥的机制相比，摘要认证所提供的认证机制就不够强。同样，摘要认证除了能保护密码外，并没有提供保护其他内容的方式——请求和应答中的其余部分仍然可能被窃听。

注 3：随着 SSL 加密 HTTP 的流行和广泛采用，有关摘要认证的现实意义曾有过很激烈的争论。时间将会告诉我们摘要认证能否达到所需的规模。