- 预先计算的词典攻击

  这是词典攻击和选择明文攻击的组合。首先，发起攻击的服务器会用预先确定的随机数和常见密码的变化形式产生一组响应，创建一个词典。一旦有了规模可观的词典，攻击服务器或代理就可以完成对流量的封锁，向客户端发送预先确定的随机数。攻击者从客户端得到一个响应时，会搜索生成的词典，寻找匹配项。如果有匹配项，攻击者就捕获了这个用户的密码。

- 批量暴力型攻击

  批量暴力型攻击的不同之处在于计算密码的方式。它没有试图去匹配预先计算出来的摘要，而是用一组机器枚举了指定空间内所有可能的密码。随着机器运行速度变得越来越快，暴力型攻击的可行性也变得越来越强了。

总之，这些攻击所造成的威胁是很容易应对的。防止这些攻击的一种方法就是配置客户端使用可选的 cnonce 指令，这样响应就是基于客户端的判断产生的，而不是用服务器提供的随机数（这个随机数可能会被攻击者入侵）产生的。通过这种方法，再结合一些强制使用合理强密码的策略，以及一个好的密码过期策略，就可以完全消除选择明文攻击的威胁。

13.5.7 存储密码

摘要认证机制将对比用户的响应与服务器内部存储的内容——通常就是用户名和 H(A1) 元组对，其中 H(A1) 是从用户名、域和密码的摘要中导出的。

与 Unix 机器中传统的密码文件不同，如果摘要认证密码文件被入侵了，攻击者马上就能够使用域中所有文件，不需要再进行解码了。

消除这个问题的方法包括：

- 就像密码文件中包含的是明文密码一样来保护它；
- 确保域名在所有域中是唯一的。这样，如果密码文件被入侵，所造成的破坏也只
305 局限于一个特定的域中。包含主机和 domain 的全路径域名就可以满足这个要求。

尽管摘要认证提供的解决方案比基本认证要强壮且安全得多，但它并没有为内容的安全提供任何保证——真正安全的事务只有通过 SSL 才能实现，我们将在下一章介绍。

13.6 更多信息

更多有关认证的信息，参见以下资源。

- http://www.ietf.org/rfc/rfc2617.txt

RFC 2617，“HTTP Authentication：Basic and Digest Access Authentication.”
306 （“HTTP 认证：基本和摘要访问认证”）。