下面来看看摘要认证的工作原理(这是一个简化版本)。

- · 在图 13-1a 中, 客户端请求了某个受保护文档。
- · 在图 13-1b 中, 在客户端能够证明其知道密码从而确认其身份之前, 服务器拒绝 提供文档。服务器向客户端发起质询,询问用户名和摘要形式的密码。
- 在图 13-1c 中,客户端传递了密码的摘要,证明它是知道密码的。服务器知道所 有用户的密码,5因此可以将客户提供的摘要与服务器自己计算得到的摘要进行 比较, 以验证用户是否知道密码。另一方在不知道密码的情况下, 很难伪造出正 确的摘要。
- 在图 13-1d 中,服务器将客户端提供的摘要与服务器内部计算出的摘要进行对比。 如果匹配、就说明客户端知道密码(或者很幸运地猜中了!)。可以设置摘要函 数,使其产生很多数字,让人不可能幸运地猜中摘要。服务器进行了匹配验证之 后,会将文档提供给客户端——整个过程都没有在网络上发送密码。

(a) 请求 因特网 请将内部销售额预测发给我 客户端 服务器 你请求的是一个保密的财务文档。 (b) 质询 因特网 请告知用户名和密码摘要。 客户端 服务器 询问用户名和密码 digest("Ow!") = A3F5 请将内部销售额预测发给我。我的用 (c) 授权 因特网 户名为"bri", 我的密码摘要为"A3F5" 客户端 服务器 digest("Ow!") = A3F5 匹配! 好的。你发送过来的搞要与我存储的 (d) 成功 因特网 密码摘要相匹配,这是你要的文档。 客户端 服务器

图 13-1 用摘要来实现隐藏密码的认证

287

注 4. 有一些技术、比如词典攻击、会首先尝试一些常见的密码。这些密码分析技术可以极大地简化密码破 译讲程。

注 5: 实际上,服务器只需要知道密码的摘要即可。