(4) 基本认证没有提供任何针对代理和作为中间人的中间节点的防护措施，它们没有修改认证首部，但却修改了报文的其余部分，这样就严重地改变了事务的本质。

(5) 假冒服务器很容易骗过基本认证。如果在用户实际连接到一台恶意服务器或网关的时候，能够让用户相信他连接的是一个受基本认证保护的合法主机，攻击者就可以请求用户输入密码，将其存储起来以备未来使用，然后捏造一条错误信息传送给用户。

这一切说明，在友好的环境，或者说是希望有隐私保护但隐私保护并不十分必要的环境中，可以通过基本认证来提供便捷的文档个性化服务或访问控制保护。通过这种方式，可以用基本认证来防止一些好奇的用户无意中或不小心对文档进行访问。[1]

比如，在一个公司内部，产品管理可能要对未来的产品计划进行密码保护，以防止信息的过早发布。对一般用户而言，基本认证就足以让他们感到不便而不会再去访问这些数据了。[2] 同样，你可能会用密码来保护那些并非高度机密的，或者没什么信息价值的私人照片或私有站点，这些信息确实和其他人也没什么关系。

将基本认证与加密数据传输（比如 SSL）配合使用，向恶意用户隐藏用户名和密码，会使基本认证变得更加安全。这是一种常用的技巧。

我们会在第 14 章讨论安全加密技术。下一章将介绍更复杂的 HTTP 认证协议——摘要认证，摘要认证具有比基本认证更强的安全特性。 284

12.4 更多信息

更多与基本认证和 LDAP 有关的信息，请参见以下资源。

- http://www.ietf.org/rfc/rfc2617.txt
  RFC 2617，“HTTP Authentication：Basic and Digest Access Authentication.”（“HTTP 认证：基本和摘要访问认证”）

- http://www.ietf.org/rfc/rfc2616.txt 285
  RFC 2616，“Hypertext Transfer Protocol-HTTP/1.1.”（“超文本传输协议——HTTP/1.1”。）

注 1：小心，基本认证中使用的用户名和密码要有别于你在更安全的系统中所使用的密码，否则恶意用户就可以用它们来攻破你的安全账户了！

注 2：尽管不是非常安全，但公司内部的员工通常也没有太大的动力去恶意捕获这些密码。这也说明，公司确实会有间谍，也确实会有不满，想要报复的员工，所以，明智的做法是对一旦被恶意获取就会造成很大损害的数据应用更安全的策略。