

12.3	基本认证的安全缺陷	300
12.4	更多信息	301
第 13 章 摘要认证		303
13.1	摘要认证的改进	304
13.1.1	用摘要保护密码	304
13.1.2	单向摘要	306
13.1.3	用随机数防止重放攻击	307
13.1.4	摘要认证的握手机制	307
13.2	摘要的计算	308
13.2.1	摘要算法的输入数据	308
13.2.2	算法 $H(d)$ 和 $KD(s,d)$	310
13.2.3	与安全性相关的数据 (A1)	310
13.2.4	与报文有关的数据 (A2)	310
13.2.5	摘要算法总述	311
13.2.6	摘要认证会话	312
13.2.7	预授权	312
13.2.8	随机数的选择	315
13.2.9	对称认证	315
13.3	增强保护质量	316
13.3.1	报文完整性保护	316
13.3.2	摘要认证首部	317
13.4	应该考虑的实际问题	317
13.4.1	多重质询	318
13.4.2	差错处理	318
13.4.3	保护空间	318
13.4.4	重写 URI	319
13.4.5	缓存	319
13.5	安全性考虑	320
13.5.1	首部篡改	320
13.5.2	重放攻击	320
13.5.3	多重认证机制	320
13.5.4	词典攻击	321
13.5.5	恶意代理攻击和中间人攻击	321
13.5.6	选择明文攻击	321
13.5.7	存储密码	322
13.6	更多信息	322
第 14 章 安全 HTTP		323
14.1	保护 HTTP 的安全	324
14.2	数字加密	326