Advanced Computer Networks

Homework 4

Assigned: May 24, 2013

Due: May 31, 2013

1. One mechanism for resisting replay attacks in password authentication is to use one-time passwords: A list of passwords is prepared, and once password[N] has been accepted the server decrements N and prompts for password[N-1] next time. At N = 0 a new list is needed. Outline a mechanism by which the user and server need only remember one master password *mp* and have available locally a way to compute *password[N] = f(mp,N)* . Hint: Let g be an appropriate aone-way function (e.g., MD5) and let $\text{password[N]} = g^N(\text{mp}) = g$ applied N times to mp . Explain why knowing password[N] doesn't help reveal password[N-1]. (q6 Chapter 8 Peterson and Davie)

2. Consider the following simple UDP protocol (based loosely on TFTP, RFC1350) for downloading files:
   - Client sends a file request.
   - Server replies with first data packet.
   - Client sends ACK, and the two proceed using stop-and-wait

   Suppose client and server possess keys K_C and K_S, respectively, and that these keys are known to each other.

   (a) Extend the file downloading protocol, using these keys and MD5, to provide sender authentication and message integrity. Your protocol should also be resistant to replay attacks.

   (b) How does the extra information in your revised protocol protect against the arrival of late packets form prior connection incarnations and sequence number wraparound? (q13 Chapter 8 Peterson and Davie)