University of California, Berkeley
College of Engineering
Department of Electrical Engineering and Computer Science Department

CS 194 S. Shenker
Spring 2005 I. Stoica

Homework Assignment #3— Due: April 18, 2005 @ 11:59:59pm

Total: 8 points

1. (**4 points**) Problems from Tanenbaum & Steen book. (1 point for each problem)
   a. Chapter 9 – Problem 3 (page 573)
   b. Chapter 9 – Problem 15 (page 573)
   c. Chapter 10 – Problem 9 (page 645)
   d. Chapter 10 – Problem 14 (page 645)

2. (**2 points**) Assume a client A that asks server S to execute an operation O. Instead of executing operation O itself, S wants to **delegate** this operation to another server S1. Give a simple authentication protocol which allows S to **securely** delegate operation O to S1. In particular, this protocol should:
   1. allow S to inform client A of server S1;
   2. allow A to verify that the server A connects to is indeed server S1 trusted by S (i.e., precludes a man-in-the-middle attack to redirect the traffic of A to another server S2).

3. (**2 points**) Lecture 14 shows an algorithm to securely admit a new member in the group. Give a protocol to securely **remove** a member from the group.

Hint: Observe that the remaining members in the group can no longer use the shared secrete key C_{KG}, since this key is known by the member who left, and this member can no longer be trusted.