Homework 5

Due: June 6, 2016 (**Revised due date**; note this is a Monday) **Points:** 100

Questions

Remember to justify your answers.

1. (*40 points*) Needham and Schroeder suggest the following variant of their protocol:

   1. Alice → Bob : Alice
   2. Bob → Alice : $\{ \text{Alice} \,||\, rand_3 \}\, k_{Bob}$
   3. Alice → Cathy : $\text{Alice} \,||\, \text{Bob} \,||\, rand_1 \,||\, \{ \text{Alice} \,||\, rand_3 \}\, k_{Bob}$
   4. Cathy → Alice : $\{ \text{Alice} \,||\, \text{Bob} \,||\, rand_1 \,||\, k_{session} \,||\, \{ \text{Alice} \,||\, rand_3 \,||\, k_{session} \}\, k_{Bob} \}\, k_{Alice}$
   5. Alice → Bob : $\{ \text{Alice} \,||\, rand_3 \,||\, k_{session} \}\, k_{Bob}$
   6. Bob → Alice : $\{ rand_2 \}\, k_{session}$
   7. Alice → Bob : $\{ rand_2 - 1 \}\, k_{session}$

   Show that this protocol solves the problem of replay as a result of stolen session keys.

2. (*20 points*) Does using passwords with salts make attacking a specific account more difficult than using passwords without salts? Explain why or why not.

3. (*30 points*) A vendor advertises that its system was connected to the Internet for 3 months, and no one was able to break into it. It claims that this means the system cannot be broken into from any network.

   (a) Do you share the vendor's confidence? Why or why not?

   (b) If a commercial evaluation service had monitored the testing of this system and confirmed that, despite numerous attempts, no attacker had succeeded in breaking into it, would your confidence in the vendor's claim be increased, decreased, or unchanged?

4. (*10 points*) Please complete the survey on secure programming at `https://purdue.qualtrics.com/SE/?SID=SV_9BPGWUWwdNhN0s5`. Your answers to the questions in the survey will not be graded; you will receive credit simply for filling out the survey. Further, the instructor will not know how you answered any of the questions.

Extra Credit

5. (*20 points*) The year 2038 will pose a problem for most 32-bit Linux systems because of the way time is represented. What specific aspect of the representation makes that year a problem? When during the year does the problem occur? Give a specific date and time. Show how you got it. What is the date with the same effect on a 64-bit system?
   Hint: You will need to write a small program to find the specific date and time.