CSci 530 Midterm Examination (Fall 2004)

Instructions: Instructions: Show all work. If a question asks for a numerical or algebraical result, indicate your answer clearly (for example, by drawing a box around it). No laptop computers are allowed; handheld calculators are permitted. This exam is open book, open notes. You have 90 minutes to complete the exam. Please prepare your answers on separate sheets of paper. You may write your answers on the sheet of paper with the question (front and back). If you need more space, please attach a separate sheet of paper to the page with the particular question. Do NOT extend your answer on the back of the sheet for a different question, and do NOT use the same extra sheet of paper to answer more than one question. In particular, each numbered questions must appear on separate pieces of paper so that the exam can be split for grading. Be sure to include your name and USC ID number on each page. There are 100 points in all and 4 questions

1. (20 points) Which of the following cryptosystems are vulnerable to brute force key guessing attacks?
    - a. RSA (1 point)
    - b. One time pad (1 point)
    - c. DES (1 point)
    - d. AES (1 point)
    - e. (6 points) For each of the cryptosystem that you have said are vulnerable, what does the attacker need to validate his or her guess.
    - f. (6 points) In which cases above does the vulnerability present a significant real weakness, and in which cases is it primarily theoretical. Explain your answer.
    - g. (4 points) What steps can be taken to minimize the effectiveness of key guessing such attacks.
2. (20 points) Key Storage and Management
    - a. (4 points) List 4 substantially different (e.g. floppy disk, USB disk and compact flash memory cards count as only one alternative) alternatives for storage of encryption keys, password, or key like information, including at least one approach that is resistant to disclosure to malicious software.
    - b. (16 points) Describe the advantages and potential weaknesses of each approach you have listed.
3. (30 points) Explain the difference in data protection provided by SSL as compared with that provided by PGP or S/MIME. Be sure to touch upon each of the issues below:
    - a. (10 points) Which basic protections are (or may be optionally) provided from among: access control, audit, authentication, confidentiality, and integrity. (Answer as yes/no for each, and if yes, one sentence describing the protection provided).
    - b. (5 points) Persistence of the protections you listed in part a. By this I mean, for how long do the protections hold?
    - c. (5 points) What are and where do the weaknesses lie in the protections provided by each approach.
    - d. (10 points) Discuss the performance and complexity impact for the management of the protections listed in your answer to part a. Discuss the tradeoff between performance and management as compared with persistence and strength of the assurances provided.
4. (30 points) Design question:
   You have been hired by a consortium of banks to help them solve the phishing problem. You have been asked to provide them with a rough sketch for three initiatives, a short term user education initiative that can be launched right away, a mid-term initiative that can involve deployment of technology in browser plug-ins, and eventually the browsers themselves, and a longer term technology intensive initiative that will be more effective, but which might cost more and require a longer technology deployment cycle.
    - a. (10 points) What will customers be told in the education initiative. What steps should they take to keep from becoming a victim? How will you notify the customers?
    - b. (10 points) What changes can be made to browsers, and what infrastructural components can be extended to better identify attempted identity theft using "phishing" attacks. What weaknesses are present in your approach (consider other approaches to identity theft beyond just "phishing".
    - c. (10 points) What is needed to effectively solve the identity theft problem in an open computing environment like today's Internet. What solution would you deploy? What would be the greatest obstacles to deployment of your approach?