CSci 530 Final Examination (Fall 2003)

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 computers are allowed; handheld calculators are permitted. This exam is open book, open notes. You have 2 hours to complete the exam. There are 100 points in all. Answer each problem on the sheet of paper on which it is printed.(That is, answer question 1 on page 1 and 2, question 2 on pages 3 and 4, and so forth. If you need more space to answer any of the questions, attach a separate sheet of paper for each such question, and clearly indicate which question is answered on each attached sheet. To ensure proper grading, please write your name on all sheets of the exam (including those you attach,if any).

Name:

1. (8 points each, 24 points total)

   (a) In RSA, what (if anything) is indicated if a plaintext x encrypts to a ciphertext y, and plaintext y encrypts to ciphertext x? Give values of e, d, and n that yield this curious situation. What are the problems associated with using such values?

   (b) In a Feistel network, the block is broken into two halves, and the output is computed from the input according to the formula

   $$L_i = R_{i-1}$$
   $$R_i = L_i \oplus f(R_{i-1}, K_i)$$

   where the K_i are the subkeys and f is an arbitrary function. Show that the structure of a Feistel network guarantees that the same process can be used for both encryption and decryption, provided that some small modifications are made. What are these modifications? (Hint: $(A \oplus B) \oplus B = A$)
   (c) A document is typically digitally signed by hashing it down to a short sequence of bytes typically 16 or 20 bytes), then encrypting that sequence with the signer��s private key. What are the benefits of performing the hash before the encryption? What are the risks?

2. (10 points each, 20 points total)

   (a) In class, we discussed CISL and IDMEF, two frameworks for exchanging information about intrusions and their effects between components of a distributed intrusion detection system. What concerns might a secure transport system for either framework have to contend with?

   (b) Explain what an access control matrix is, and how it is actually implemented. What factors in authorization would not be well expressed in an access control matrix?

3. (26 points total)

   (a) (16points) What are the similarities and differences between signature-based and anomaly-based intrusion detection?What are the strengths and weaknesses of both? Which would you choose,and why,for detecting attacks in each of the following cases:

i. A popular e-mail client.
ii. An experimental high-performance network with few users.
iii. A web server for a high-volume web site.

(b) (10 points) In some sense, the two kinds of intrusion detection seem to be diametrically opposed. Is this a false dichotomy - that is, are there (or can there be) methods for intrusion detection that don��t employ either technique or a mixture of the two? Explain.

4. (30 points) You have been hired as a consultant to advise on the design of a security mechanism that will be used to protect patient data in a new medical records system. This system will manage and support the transmission of patient records, including very large images files for X-rays, MRI, CAT-scans and other procedures. The system must provide appropriate levels of protection to meet HIPAA privacy regulations, and it must allow the access to records needed by physicians and specialists to which patients are referred.

   (a) Describe appropriate requirements for confidentiality, integrity, accountability,and relibility/availability in such a system.

   (b) In what part(s) of the system (e.g.,where in the protocol stack would you include support for each of the requirements identified in (a)? Why would you place mechanisms where you suggested; what were the issues you considered?

   (c) What security mechanisms and approaches to implement those mechanisms would you use to meet the requirements
   in (a) as implemented in the parts of the system you identified in (b)?