Print FAMILY name, first initial:__________________________

Examination 1

CEN 5540 Computer and Network Security

10 October 2002

Instructions Read all instructions. Failure to follow instructions will result in loss of points.

1. This is a closed-book examination.
2. You are permitted one 8.5 by 11 inch sheet of notes, both sides, that you have prepared.
3. You are permitted 50 minutes to complete this examination.
4. **Do not start** the exam until the proctor has told you to start.
5. **Answer any two (2) questions, and no more.** All questions are of equal value.
6. **Leave sufficient room in the upper lefthand corner for the staple** and staple your answer sheets in the room you have left.
7. Start the answer to each question on a new page (i.e., do **not** put the answer to more than one question on the same page).
8. Use exactly one page of paper (both sides is OK) to hold the answer to each question, and please write legibly.
9. Show your work.
10. Put the question number in the top center of each answer page and label each part of the question answer.
11. Include your last name and page number in the upper right hand corner of each answer page.
12. Assemble your answers in numerical order of the questions when you submit them.
13. Print your family name and first initial in the upper right hand corner of this page, and complete the honor statement affirmation below.

Read and sign the following statement. This page **MUST** be attached to your examination answers and **MUST** be completed to obtain credit for this examination.

On my honor, I have neither given nor received unauthorized aid on this examination.

Signed:

Printed Name:

SSN:

1. (a) (6) Give practical examples illustrating the meanings of the following principles:

    i. Principle of Efficetiveness

    ii. Principle of Adequate Protection

    iii. Principle of Easiest Penetration

    iv. Belt and Suspenders

    How do these principles inform our efforts to provide security in information systems?

   (b) (9) Relate the four main threat types to the three main goals of security.

2. (a) (8) Consider a computer system to which an attacker has physical access. Give three OS controls that the attacker will be able to overcome easily, and one control that will be more difficult to circumvent. Justify your answers.

   (b) (4) Describe how the basic fetch-decode-execute microprocessor cycle must be modified if the system uses a tagged architecture. When and how should the tag bits be set, assuming they are used for content type (data/instruction, read-only/read-write)?

   (c) (3) What type of virtual memory would be most appropriate for tagging at the memory block level, and why? How would this change the checks in the fetch-decode-execute cycle?

3. (a) (5) What are the fundamental differences between a boot sector virus and an application document virus?

   (b) (2) Why is it that we see more application document viruses and fewer boot sector viruses than we used to?

   (c) (4) Describe two ways to detect viruses statically, and how a virus might be able to circumvent these detection methods.

   (d) (4) Describe the four distinct methods used by the Internet Worm to infect other hosts.

4. (a) (3) Argue for or against the statement that covert channels are only a concern for systems with mandatory access controls.

   (b) (6) Draw the state transition diagram and label the arcs for a covert timing channel involving detection of CPU usage. Assuming that reading the system clock takes 200 microseconds, a context switch takes 300 microseconds, that the round robin time quantum is 2 milliseconds, and that all other operations take negligible time, what is a rough estimate of the channel capacity, assuming that an equal number of zeros and ones are sent?

   (c) (6) Using the SRM, complete the table below to show possible information flows. Indicate these by inserting a small 'r' in the cells where the flow may occur. What must be done after this inital step of the SRM is done to complete management of covert channels? Why?

Resource	P1	P1	P3	P4
R1				R
R2			R	
R3		R	R	M
R4	R		M	
R5	M	R		
R6				R

5. (a) (5) How do commercial policies differ from the strict information flow policies? Why?

   (b) (4) Show how a lattice model can implement a Chinese Wall policy.

   (c) (2) Relate the SRM to the BLP model.

   (d) (4) Show that the cross product of two lattices with the order relation extended by dominance produces a new lattice.

6. (a) (3) In what ways did the Orange Book succeed, and in what ways did it fail?

   (b) (5) How did the Green Book improve on the Orange Book? Why are these improvements significant?

   (c) (3) What contribution did the British Evaluation make to the Common Criteria? Why is this important?

   (d) (4) What are the differences between a PP, an ST and a TOE in the Common Criteria?