Last Name:

Examination 1
CEN 5540 Computer and Network Security
30 May 2000

Instructions:

- **Failure to follow instructions may result in loss of points.**
- Do not start the examination until instructed to do so.
- This test is closed book, but you may use one 8.5" by 11" sheet of notes you have prepared.
- **Answer three (3) questions below.**
- 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).
- Show your work.
- Assemble your answers in numerical order of the questions when you submit them.
- **Leave a 1" square in the upper left corner for a staple.**
- Be sure to include your name on your answer sheets.
- You have 60 minutes to complete this examination.
- **Read and sign the following statement.** You may write this on your exam and sign it there if you wish to take the exam questions home with you today. Do not discuss this exam with anyone in this course who has not yet taken this exam.

On my honor, I have neither given nor received unauthorized aid on this examination, and I will not discuss the contents of this examination with any student who has not yet taken this examination.

Signed:

1. (a) (4) In what ways do the three basic goals of information security overlap?
   (b) (5) Why are the added goals of authenticity and non-repudiation often added when network security is considered, but not computer security? How do these goals differ from each other?
   (c) (6) Describe three different controls to reduce the threat of login spoofing trojan horse programs. Indicate how they are effective and any shortcomings.

2. (a) (6) What are the differences between a boot sector virus, an application virus, and a macro virus? Consider what each must do to spread and how they may be controlled.
   (b) (2) Why are viruses more prevalent on PCs than on multiuser systems?
   (c) (2) The LoveBug code has been called a virus and a worm. Which would you call it and why?
   (d) (5) How did the Internet Worm spread, and what types of flaws allowed this to occur?

3. (a) (6) What is involved in configuration management? How does this improve security in system development?
   (b) (3) Where should separation of duty be part of software development policy, and why?
   (c) (6) Show how the SRM method could detect the presence of a covert channel using disk system exhaustion.

4. (a) (3) Reading the system clock is generally treated as an unprotected operation, but in some systems it is protected. Why?
   (b) (5) What are the strengths and weaknesses of biometric authentication techniques? Be thorough and specific.
   (c) (4) Why are setuid programs considered a greater security risk than servers providing the same types of access?
   (d) (3) Why are domains also considered as objects in the ACM?

5. (a) (3) Compare and contrast security and trust.
   (b) (3) Compare and contrast certification and accreditation.
   (c) (4) Describe a shortcoming in the Clark-Wilson policy, and give some extensions that could address this limitation.
   (d) (3) What are the main differences between the four main categories of trusted systems under the TCSEC?
   (e) (2) What are the main contributions that the German Green Book made to thought regarding evaluation?