Last Name:

Examination 1
CEN 5540 Computer and Network Security
3 April 2001

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 two (2) 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).
- Put the question number in the middle of the top of each answer 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 50 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) What is social engineering? How is it used? What controls are there for it, and how are they effective?

   (b) (8) List four controls for computer viruses, describe how and why each works, and for each, illustrate how a virus might be able to render the control ineffective.

   (c) (3) Why is static analysis of code limited in its ability to detect malicious programs?

2. (a) (6) What elements of the operating system have to be protected and in what ways? Show how compromise of each protected part could lead to compromise of other parts.

   (b) (2) Give an example of how compartmented authorization within the operating system could be used to reduce one of the risks you give for the previous part.

   (c) (3) Draw the state machine diagram for a covert channel that uses the following mechanism. High signals Low by the existence (1) or non-existence (0) u of a file in a system that returns different error codes for a failed file open call for the cases in which the file exists but the caller has inadequate permissions, and the case in which the file does not exist.

   (d) (4) Estimate the maximum channel capacity of the covert channel described in the previous part. File creation takes 1200 microseconds, file deletion takes 800 microseconds, successful file open takes 600 microseconds, unsuccessful file open takes 500 microseconds, and context switches take 250 microseconds. Show your work.

3. (a) (3) What is trusted path in the Trusted Computing System Evaluation Criteria (TCSEC), and why is needed?

   (b) (12) Compare the pros and cons of the following four trust models for software distribution:

      i. code comes with a cryptographic seal and signature by the vendor;

      ii. code comes with assertions of its behavior along with proofs that can be checked with an automatic theorem checker;

      iii. code comes with assertions of its behavior that are cryptographically sealed and signed along with the code by a third party;

      iv. code comes with nothing but is monitored by the system as it runs to check for bad behavior.

4. (a) (3) What is the primary difference between the C levels of the TCSEC and the B levels? Between the B3 level and the A1 level?

   (b) (3) In the Common Criteria (CC), what is the smallest coherent set of mechanisms called?

   (c) (3) How does and EAL in the CC relate to the German Green Book?

   (d) (6) Distinguish a Protection Profile from a Security Target from a Target of Evaluation. What does an ST have that a PP does not, and why?